(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35253 A1

(51) International Patent Classification[7]: G06F 17/00, 17/30, 13/00, 12/00, H04L 9/00

(21) International Application Number: PCT/US00/30671

(22) International Filing Date: 8 November 2000 (08.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/164,141	8 November 1999 (08.11.1999)	US
60/179,125	31 January 2000 (31.01.2000)	US
60/179,066	31 January 2000 (31.01.2000)	US
60/200,890	28 April 2000 (28.04.2000)	US
60/200,884	1 May 2000 (01.05.2000)	US
60/206,333	23 May 2000 (23.05.2000)	US
09/614,344	12 July 2000 (12.07.2000)	US

(71) Applicant: USERTRUST, INC. [US/US]; 265 East 100 South, Salt Lake City, UT 84111 (US).

(72) Inventor: TOSCANO, Paul; 941 East Tahnia Park Circle, Salt Lake City, UT 84121 (US).

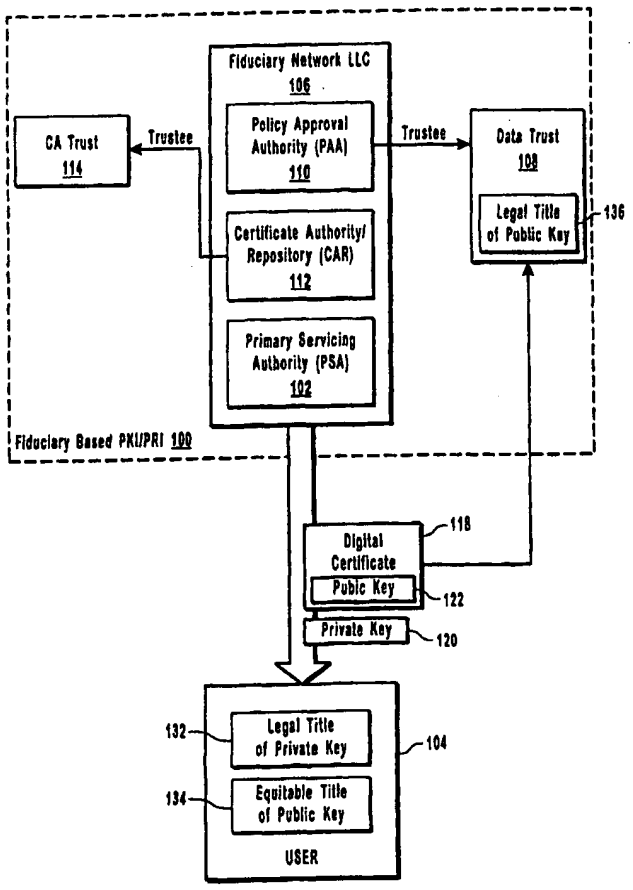
(74) Agents: ISRAELSEN, R., Burns__ et al.; Workman, Nydegger & Seeley, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

[Continued on next page]

(54) Title: LEGAL-BASED OR FIDUCIARY-BASED DATA MANAGEMENT PROCESS



(57) Abstract: Informational Privacy and Public Keys of users are protected by a Privacy Architecture having a PKI and/or PRI function (100). The Privacy Architecture protects the Informational Privacy (120) and Public Keys (122) using physical security measures combined with trusts that result in protector or fiduciary duties being owned to the users (104). The users of public keys and repository services become beneficiaries of the trust, such that they are owed a fiduciary duty by its trustees. The second trustee holds encryption and repository security technology in trust for the first trustee. Thus, users have the double protection of two or even more trustees. If there is only one trustee, it assumes the responsabilities otherwise assigned to the first and second trustees. The Privacy Architecture includes a profit-making entity in the form. The responsabilities of establishing and implementing security fall principally to the trustee(s) rather than the profit-making entity.

WO 01/35253 A1

patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *With international search report.*

LEGAL-BASED OR FIDUCIARY-BASED DATA MANAGEMENT PROCESS

BACKGROUND OF THE INVENTION

1. The Field of the Invention

The present invention relates to systems and methods for establishing security, integrity and privacy for electronic and digital data and information (hereinafter "Information"). More specifically, the present invention relates to systems and methods operating in a technological and legal environment in which Information is protected by encryption and other technological processes and also by legal and/or fiduciary duties (hereinafter jointly and severally "fiduciary duties") such that full security, reliability, integrity and Informational privacy are achieved. A non-limiting example of a legal duty that is included in the term "fiduciary duties" is a protector duty.

2. The Prior State of the Art

As personal computers and the Internet have become more widely used, the need to cost-effectively safeguard informational privacy while preserving security, reliability and integrity of Information has increased. Because of the general acceptance and use of information technology and telecommunication of Information, it is no longer practical for many individuals and businesses to record, store, and use Information without encoding the Information in a computer-usable, electronic form. The need to maintain security, privacy, reliability, and integrity of Information is particularly acute when the Information consists of personal, sensitive or privileged information, contractual obligations, trade secrets, medical data, or other restricted matter. With the advent of the Internet and other wide area networks, it is no longer practical or possible for many individuals and businesses to store all such Information locally or to avoid placing such Information on communication media associated with the Internet or other wide area networks. These developments have resulted in a greater need for informational security, privacy, reliability, and integrity (hereinafter collectively referred to as "Informational Privacy").

twin key pair is not compromised and technological safeguards are not breached or are not rendered obsolete by more recent technological developments and advancements.

Confidentiality of Information. Confidentiality of Information can be achieved by encrypting the Information with the public key of an asymmetrical twin key pair. Again, conventional technology has been used to adequately establish confidentiality. However, such technological approaches are valid only as long as the technological safeguards are not breached or are not rendered obsolete.

Proprietary Utility of Information. While conventional methods for assuring Informational Privacy have been successful in maintaining separateness and confidentiality of Information, at least in the short term, these methods do not adequately assure the proprietary utility of Information for two basic reasons. First, because advances in technology occur rapidly and often without public knowledge, there is no certainty that the currently available encryption and security technology securing Information is in fact capable of securing it against technological advancements that render such security obsolete or subject it to compromise or attack. Second, because such technology can be rendered obsolete or insecure, it cannot over indefinite time periods guarantee the identity of the Originator, nor the date and time of origin, nor the non-reputability of the signatory of, nor the persistence of content and form of the Information; in short, it cannot guarantee the reliability or integrity of such Information. Without such a guarantee, it is impossible to ensure adequately that the utility, obligations, benefits, and burdens of the Information as established by its Originator(s), will continue to be borne over indefinite periods of time solely by the parties intended by the Originator(s). Without the assurance of Information integrity, the utility, obligations, benefits, and burdens established by the Information are not reliable over indefinite periods of time; consequently, parties cannot rely upon the Information to memorialize or establish such utility, obligations, benefits, or burdens. Without such integrity and reliability many transactions and documents that now have some paper component will not be susceptible to trustworthy digital processing and the efficiency and convenience of Internet and wireless transmission capability will not be fully realized. Assuring to Originators all the elements of Informational Privacy (separateness, confidentiality, and proprietary utility) will preserve the right

of privacy of Originators and other parties relying on such Information, while providing them enhanced expectations of privacy in such Information.

The right of privacy in Information includes the right of a person to be free from invasion of privacy in the form of

a) appropriation of the person's name or likeliness;

b) intrusion upon a person's solitude or seclusion including eavesdropping on communications and persistent unwanted communications;

c) public disclosure of private facts including highly objectionable public airing of private information even if true; and

d) disclosing Information that puts a person in false light in the public eye.

An expectation of privacy in Information means the reasonable expectation that Information will not, knowingly and without lawful authority and the consent of the Originator, sender or receiver, or be viewed, altered, intercepted, copied, confiscated, or divulged.

"Fair information practices" are rules governing the collection, storage, processing, retrieval and use of digital and electronic data and Information according to standards that protect personal and sensitive Information against abuse, unauthorized disclosure, or use, and invasion of privacy.

SUMMARY OF THE INVENTION

The present invention relates to structures, processes, systems and methods for establishing full Informational Privacy using a combination of data encryption and other technological processes in an environment in which parties with fiduciary duties safeguard and assure the components of Informational Privacy. Establishing Informational Privacy in this manner assures Originators that Information can be maintained with a high degree of certainty. When the Originator(s) are doctors, lawyers, accountants, therapists, or other individuals or organizations that have a fiduciary duty to maintain the secrets or confidences of clients or patients, the same level of care attaches to the Information when it is stored or processed by the structures, processes, systems and methods of the invention, thereby enabling such Originator(s) to be willing to avail themselves fully of Internet and wireless transmissions of Information.

The invention achieves all three elements of Informational Privacy. In doing this, the invention assures security and integrity of Information, creates and enhances the expectation of privacy and preserves the right of privacy in the Information. This is so because the invention creates a mechanism that establishes with greater certainty the identity of the Originator, the date and time of origin, the identity of parties with access rights to the Information, the identity of any signatory, the persistence of content and form of the Information, and an auditable record of the reposing, access, and retrieval or Information (hereinafter "chain of custody") over indefinite periods of time. The invention accomplishes all this because it allows Information to be entrusted with unbiased, third-party, fiduciary custodians acting apart from any profit motive and pursuant to independently promulgated policies, procedures, protocols, and practices for creating and maintaining Informational Privacy.

The present invention guarantees Informational Privacy in ways that cannot be achieved using only transmission security measures, high-grade encryption (e.g., digital certificates), and other security technologies. Informational Privacy in Information arising in commercial, legal, professional, or other sensitive arenas can be guaranteed according to the invention to at least ensure with respect to such Information that:

1) the Originator, signatory(ies), or parties with access rights are known and linked to the document;
2) Information access is controlled and subject to the requirements of authorized parties;
3) the Information is rendered tamper-proof even against Originators, signatories, parties with access rights, senders, and receivers;
4) the Information is rendered persistent both as to form and content over indefinite periods of time;
5) the origin and chain of custody of Information are rendered traceable;
6) the evidentiary integrity of Information in a court of law or equity is preserved;
7) the trustworthiness of Information is certifiable by its neutral and trusted third-party custodian; and

8) the long-term reliability of Information is ensured in spite of technological advances, changes in law, or disputes among those directly affected by the Information.

The absence of these guarantees has substantially hindered the widespread acceptance of the Internet and wireless transmission in certain industries and professions. By addressing and overcoming these shortcomings that cannot be remedied or overcome by conventional security measures, the invention disclosed herein provides the last components necessary to enable the highest and best use of Information in a wide range of arenas including but not limited to commercial, legal, medical, educational, and industrial contexts.

Informational Privacy is established according to the invention by a legal and/or fiduciary network of entities (hereinafter "Network") in which the rights and duties for establishing security policies, implementing the security defined by the security policies, and engaging in profit-making activities are enumerated and divided among the entities of the Network according to an operational agreement. Separating the various responsibilities among different entities of the Network ensures that the profit-making entity does not have conflicting interests that might lead to security breaches or abuses.

In one implementation of the invention, the Network that provides data transmission, storage, and processing services includes one or more non-profit corporations, each of which is a fiduciary (hereinafter "trustee(s)") for one or more fiduciary entities (hereinafter "trust(s)") associated with the Network. In the event there is but one trust and its trustee, this trust exits to promulgate Network policies, procedures, protocols, and practices. In the event there are more than one trust and trustees, then the first trustee and the corresponding trust exist to promulgate Network policies, procedures, protocols and practices. Or, in the alternative, these duties may be shared among the various trusts and trustees. These policies, procedures, protocols and practices govern (1) all aspects of administration of public key infrastructure (hereinafter "PKI") and all aspects of private repository infrastructure (hereinafter "PRI"). The policies, procedures, protocols and practices governing the PKI are contained in a Certification Practices Statement ("CPS"). The policies, procedures, protocols, and practices governing the PRI are contained in a Repository Practices

Statement ("RPS"). The CPS and RPS include Information Privacy measures that involve desired, existing or contemplated future technology. In the event the Network consists of more than one trust and its trustee, the responsibility to implement the CPS and RPS and to ensure that trust beneficiaries are provided a second bulwark of protection, even against internal subversion or compromise, may be assumed by the other trusts and trustees to assure appropriate checks and balances.

The invention incorporates one or more profit-making entities in the form, for example, of a "C" corporation. Because such profit-making entities are not charged with promulgating or implementing Information Privacy, the profit-making entity is free to engage in appropriate business activity to maximize profits for its shareholders. If the profit-making entity were to attempt to compromise Informational Privacy, the trustees included in the fiduciary network would block such activity. Moreover, the invention allows, the various trustees to perform their duties unhindered by any independent profit-making motives.

The invention may also consist of non-fiduciary entities operating in the place of trusts and trustees but that function in the same protective role as the trust or trusts and the trustee or trustees. Hereinafter the terms trust(s) will be used to refer to these entities whether or not they are fiduciary entities or non-fiduciary entities.

The invention provides the subscribers and customers of the profit-making entity(ies) who apply for purchase, or license either PKI products and services (e.g. digital certificates) or PRI products and services (e.g. repository services) with the status of protected partner or beneficiaries (hereinafter jointly and severally "beneficiaries") of the trusts. The duties owed by the trusts to such beneficiaries are superior to the duties owed to such subscribers and customers and the liabilities that would be imposed on the profit making entities if such subscribers and customers were not given the status of beneficiaries by the invention. The fiduciary duties of care guaranteed by the Invention with respect to the Information stored, transmitted, or processed pursuant to the CPS and RPS are of the same elevated nature as the fiduciary duties of doctors, lawyers, accountants, therapists, other professionals. For this reason, such professional users can be confident that Information whose Information Privacy is safeguarded by the invention will be protected at the same level of care that these professional users owe to their clients or patients.

Additional features and advantages of the invention will be set forth in the description that follows and, in part, will be obvious from the description, or may be learned by the practice of the invention. These and other features and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the present invention will become more fully apparent from the following description and appended claims or may be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to set forth how the above-recited and other advantages and features of the invention are achieved, a more particular description of the invention (briefly described above) will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. It should be understood that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope and that the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings. These drawings are as follows:

Figure 1, illustrating an exemplary system that provides a suitable operating environment for the present invention;

Figure 2A, illustrating a conventional technique for digitally signing a Information;

Figure 2B, illustrating a conventional technique for digitally signing and encrypting Information;

Figure 3, presenting a list of digital certificates associated with varying degrees of service, which can be used with the invention.

Figure 4, illustrating an example of the organizational environment in which Information can be transmitted, processed, or stored in a manner in which the Informational Privacy is achieved;

Figure 5, illustrating issuance of a digital certificate according to the invention.

Figure 6, illustrating a Network operating a legal-based or fiduciary-based public key infrastructure and private repository infrastructure, with the Network

including a plurality of certification authorities/repositories and primary servicing authorities.

DETAILED DESCRIPTION OF THE INVENTION

The present invention includes structures, processes, systems and methods that achieve Informational Privacy using legal principles and structures and scientific technologies and applications to create a joint public key/private repository infrastructure in combination to safeguard Information from breaches of security compromises of integrity and invasions of privacy by providing for such Information the protection of unbiased, fiduciary custodians operating under a system of checks and balances and responsible for safeguarding the Information under fair information policies, procedures, protocols, and practices.

1. Exemplary Processing, Transmission, and Storage Environment

Certain embodiments of the present invention include structures, processes, systems and methods that are described in reference to a special purpose or general-purpose computer comprising various computer hardware and software. Embodiments within the scope of the present invention also include computer-readable media comprising computer-executable instructions and/or data structures for performing various functions. Such computer-readable media and data storage means can be any available media that can be accessed by a general-purpose or special-purpose computer. By way of example, and not limitation, such computer-readable media and data storage means can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store executable instructions and/or data and which can be accessed by a general-purpose or special-purpose computer.

When information is transferred or provided over a network or other communications connection to a computer, the computer properly views the connection as a computer-readable medium. Thus, such a connection is also properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general-purpose computer, special-purpose computer, special-purpose processing device, or

other processor means to perform a certain function or group of functions. The computer-executable instructions and associated data structures represent an example of program code means for executing the steps of the invention disclosed herein.

Portions of the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a computer. Generally, program modules include routines, programs, objects, components, data structures, or the like that perform particular tasks or implement particular abstract data types. Those skilled in the art will appreciate that the invention may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices. The components of the foregoing computer systems that perform the computer-executable instructions are examples of processor means used in practicing the present invention.

The invention also extends to techniques whereby a computer or another processing device, in combination with the organizational and legal structures disclosed herein, receives, transmits, stores, or processes electronic information in ways that preserve full Informational Privacy. The data that is generated, transmitted, and stored, the methods for using the data, the physical activity of and the results provided by the computers, storage media, and communication media, and the various entities that use the data represent examples of useful, concrete, and tangible results associated with the invention disclosed and claimed herein.

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the invention may be implemented. The computing environment illustrated in Figure 1 represents one example of the physical environments in which data can be transmitted, processed, or stored according to the invention. Figure 1 illustrates a general purpose computing device in the form of a conventional computer 20, including a processing unit 21, a system memory 22, and a system bus 23 that couples various system components

including the system memory 22 to the processing unit 21. The system bus 23 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 24 and random access memory (RAM) 25. A basic input/output system (BIOS) 26, containing the basic routines that help transfer information between elements within the computer 20, such as during start-up, may be stored in ROM 24.

The computer 20 may also include a magnetic hard disk drive 27 for reading from and writing to a magnetic hard disk 39, a magnetic disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to removable optical disk 31 such as a CD-ROM or other optical media. The magnetic hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are connected to the system bus 23 by a hard disk drive interface 32, a magnetic disk drive-interface 33, and an optical drive interface 34, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer-executable instructions, data structures, program modules and other data for the computer 20. Although the exemplary environment described herein employs a magnetic hard disk 39, a removable magnetic disk 29 and a removable optical disk 31, other types of computer readable media for storing data can be used, including magnetic cassettes, smart cards, smarts card readers, biometric devices, tokens, flash memory cards, digital video disks, Bernoulli cartridges, RAMs, ROMs, and the like.

Program code means comprising one or more program modules may be stored on the hard disk 39, magnetic disk 29, optical disk 31, ROM 24 or RAM 25, including an operating system 35, one or more application programs 36, other program modules 37, and program data 38. A user may enter commands and information into the computer 20 through keyboard 40, pointing device 42, or other input devices (not shown), such as a microphone, joy stick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 coupled to system bus 23. Alternatively, the input devices may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB). A monitor 47 or another display device is also connected to system bus 23 via an interface, such as video adapter 48. In addition to the

monitor, personal computers typically include other peripheral output devices (not shown), such as speakers and printers.

The computer 20 may operate in a networked environment using logical connections to one or more remote computers, such as remote computers 49a and 49b. Remote computers 49a and 49b may each be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computer 20, although only memory storage devices 50a and 50b and their associated application programs 36a and 36b have been illustrated in Figure 1. The logical connections depicted in Figure 1 include a local area network (LAN) 51 and a wide area network (WAN) 52 that are presented here by way of example and not limitation. Such networking environments are commonplace in office-wide or enterprise-wide computer networks, intranets and the Internet.

When used in a LAN networking environment, the computer 20 is connected to the local network 51 through a network interface or adapter 53. When used in a WAN networking environment, the computer 20 may include a modem 54, a wireless link, or other means for establishing communications over the wide area network 52, such as the Internet. The modem 54, which may be internal or external, is connected to the system bus 23 via the serial port interface 46. In a networked environment, program modules depicted relative to the computer 20, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing communications over wide area network 52 may be used.

2. **Privacy Considerations: Personal Privacy**

The present invention achieves Informational Privacy for Originators of Information using data encryption and other security measures in combination with an organizational and legal structure that establishes and assures Informational Privacy in association with legally enforceable duties of care, fiduciary or otherwise. Prior to proceeding to a detailed description of the invention (hereinafter referred to as "Privacy Architecture™"), particularly its legal and organizational structure that achieves such Informational Privacy a discussion of some general principles relating to privacy will first be presented in order to clearly illustrate the advantages of the

invention and how such advantages cannot be achieved using conventional practices alone.

One of the basic provisions of the Privacy Architecture™ is the requirement of adherence to the CPS and the RPS (the documents that set forth the policies, procedures, and protocols associated with secure public key management and secure repository management under fair informational practices). Within the CPS and RPS as administered by the trust(s) of the Privacy Architecture™ are included the privacy, security and integrity safeguards and benefits afforded to beneficiaries of the trusts. Among the provisions of the RPS and CPS is the requirement that data protected by the Privacy Architecture™ be collected only for legally authorized purposes, by processes open to scrutiny, and only with the consent of the Originator or a party identified by the Originators, and for purposes known by or upon notice to such party and only with the data management supervision, oversight, or standards compliance audit or review of the neutral, unbiased third party trustee.

There is considerable global diversity with respect to fair information practices. The efforts of one country to create and preserve the fair treatment of sensitive Information can be thwarted by abuses taking place in other jurisdictions. Some countries restrict or prohibit data transfers to venues with insufficient protection for such Information. The European Directive governing Informational Privacy has the following objectives: 1) to ensure the rights of individuals and their right of privacy in Information, 2) to promote the free circulation within the European Community of personal data through the establishment of harmonized protection in all member states; and 3) to prevent abuse of personal data originating within the European Community by those in other countries where adequate protection is not ensured.

The United States regulates sensitive Information by narrowly defined legislation covering specific abuses in specific contexts with the goal of prohibiting abuses by government while providing minimal regulation of the private sector. Other countries, particularly the European Community, protect privacy in both public and private sectors through omnibus legislation enforceable by the state.

An analysis of actual practices in various parts of the world reveals a notable agreement on essential principles of fair information practices. The consensus can be reduced to four principles:

1) the establishment of obligations and responsibilities for creating, collecting, maintaining, processing or using personal or sensitive Information;
2) the maintenance of transparent processing of personal or sensitive Information;
3) the creation of special protections for sensitive Information; and
4) the establishment of enforcement rights and effective oversight of the treatment of personal or sensitive Information.

These four principles require that fair information practices be established to specifically ensure that personal or sensitive Information:

1) Be collected for specific stated purposes only;
2) Be used in a manner compatible with the stated purpose for its collection;
3) Be collected only to the extent necessary to accomplish the stated purpose and use;
4) Be stored only long enough to accomplish its stated purpose and use;
5) Be subject to access and correction by authorized individuals whose identity is declared in or linked to the Information;
6) Be subject to measures that ensure the integrity of the Information;
7) Be collected, processed and managed by means that are open and understandable;
8) Be subject to rules that provide special protection for sensitive Information;
9) Be subject to effective enforcement of the rights of Originators and relying parties;
10) Be subject to independent oversight;
11) Be subject to the consent of Originators and their designers; and
12) Be protected from unauthorized or abusive secondary use.

Because the private sector in the United States and in other countries does not uniformly fulfill the requirements of the four principles of fair information practices of other jurisdictions, the Privacy Architecture™ disclosed herein has been created to assure the fulfillment of these four principles and to promote the twelve basic Informational Privacy requirements listed above. The Privacy Architecture™ provides a private, non-governmental mechanism for the creation, maintenance, and adoption of uniform fair information practices that accord with and are functionally equivalent to those standards, legal and ethical, that control in other jurisdictions. By compliance with the RPS promulgated as part of the Privacy Architecture™, customers (e.g., users, subscribers, applicants, Information Originators) can adopt such fair practices and subscribe to a structural and procedural mechanism for achieving compliance with the standards of other jurisdictions.

The benefits of the Privacy Architecture™, which will be further described below, include but are not limited to:

1) Independent unbiased fiduciary or protective oversight;
2) Privacy law compliance;
3) Ownership and expectation of privacy in electronic information;
4) Restricted access;
5) User control;
6) Liability and risk management;
7) Audit of implementation of fair information practices;
8) Document Integrity ;
    a) Non-repudiation ;
    b) Evidentiary integrity;
    c) Chain of custody;
    d) Persistence of content and form;
    e) Verification of claimed ownership;
    f) Date and time stamping;
    g) Controlled access and retrieval;
    h) Tracking subsequent uses/accesses/retrievals/revisions;
9) Uniform privacy policies, procedures, practices; and
10) Protection against technological obsolescence .

As stated previously the three principal elements of Informational Privacy are (1) Separateness, (2) Confidentiality, and (3) Proprietary Utility.

1) Separateness involves (a) partitioning Information, (b) identifying it and the ownership and access rights connected to it, (c) creating or acknowledging an assertion of a justifiable claim of right to such Information, and (d) providing notice to pertinent parties of such a claim of management.

Partition is an abstract way of referring to who a person is and what belongs to the person. Partition involves separation and definition of a new entity. For example, bodily partition happens to people at birth, or fetal viability, when the fetus is seen as separate from the mother and a new human being is defined. Property is partitioned by separating it from its context and defining it in terms of new boundaries. We partition when ever we recognize the difference between the "I" and the "Thou," between "Mine" and "Thine." The first element of privacy is to separate the one from the many, to quarry out what is commingled. Once who a person is and what belongs to the person is defined, the person can take the next step and assert and justify a claim of right in what is partitioned.

The assertion and justification of a claim of right can be made either by a group or by an individual. The assertion of the claim may be to ownership, access, easement, use, exploitation, or merely to a possessory interest in the name of someone else. It can be a claim to tangible or intangible property, to non-intrusion, to a given action or omission—in short to anything that is identifiable. The justification of a claim of right can be made on any principle from adverse possession, to the divine right of kings, to the authority of religious authority, to the payment of consideration, to custom, tradition, or even to outrage.

The assertion and justification of a claim of right in what is identified or partitioned, however, cannot happen merely in one's mind. It must be declared, if not publicly, then at least before credible witnesses if the assertion is to stand and the justification tested. This declaration constitutes notice, which usually forms the basis of the next element of privacy, namely, restriction of access.

2) Confidentiality involves the restriction of access to such Information. Restriction of access is what most people think of as privacy, even though it is predicated up the elements of partition, assertion, justification, and declaration. Restriction is the "Leave Me Alone" element. Privacy is not private unless access is restricted, unless society or the individual is willing, if not ready and able, to protect a person from the claims of others, from invasion, intrusion, observation, measurement, assessment, and judgment by unwanted interlopers. Restriction is essential to the next element of privacy, proprietary utility.

3) Proprietary utility involves management of the Information such that only intended parties are burdened or benefited thereby. Proprietary utility consists of the flow only to intended parties of the benefits and burdens of whatever is partitioned, claimed, and restricted. A residence is not private if anyone can live there. Information is not private if anyone can see it, use it, or benefit from it. A contract is not private law if anyone can claim its benefits or avoid it burdens. Proprietary utility in information, electronic or otherwise, requires that the parties relying on the information have certainty with respect to informational provenance, persistence of form and content, chain of custody, evidentiary integrity -- all of which require the reliable and secure custodianship of an unbiased fiduciary with no stake in the information's form or content and which operates beyond the undue influence of public or private entities.

Provenance refers to the origin and history of information, including its source or author and date of origination. Persistence refers to the fact that the document's form and content of information are reliably fixed and cannot be altered without detection. Chain of custody refers to a traceable record of consistent custodianship of the document over indefinite periods of time. Evidentiary integrity refers to the reliability of a document as good evidence in a court of law, which often requires all of the foregoing elements.

The ultimate result of these elements of Informational Privacy is individual, personal autonomy. Autonomy is the fundamental right of individuals in open societies to acquire and expend resources, including Information, to achieve outcomes

apart from the expectations, assumptions, and aspirations of the collective, be it public or private.

Autonomy is the goal of privacy. It contemplates the unimpeded use of private resources and information to pursue self-determined ends and outcomes in the face of (individual or collective) assumptions, expectations, aspirations, obligations, pressures, threats, or outright force exercised by persons or institutions that may be indifferent to distinctions between "I and Thou," "Mine and Thine."

The heart of privacy is not merely to be let alone. The heart of privacy is the right and power to exert ones individual will and resources against those of the collective in order to challenge its assumptions, aspirations, expectations, and obligations, to chastise its elite, resist its temptations, contradict its assertions and justifications, attack its conclusions, assess its worth, audit its operations, proclaim its sins, protest its malice and indifference, engage its leaders, participate in its governance, and contribute to it one's personal influence for the common good. This is autonomy—the right to the individual to self-definition, self-determination, and the public exercise of private judgment independent of any coercive, illegal oppressive, or manipulative group power or authority.

These elements apply to personal privacy in one's body and bodily functions as much as they do to informational privacy or to the right to the quiet enjoyment of real estate.

3. Privacy Considerations: Informational Privacy

Attention is now directed to the application of privacy to Information (defined herein as information in the form of electromagnetic impulses, signals, or information stored in a computer-readable medium, either permanently or transiently). Such Information is a means of preserving human assumptions, aspirations, expectations, and obligations. The more certain and reliable this information is to users, the more valuable it is.

The principal benefit of electronic or digital Information is to facilitate transfer from one medium to another, thus making quick and cheap the processes of storage, search, access, retrieval, and use. This benefit is also its greatest drawback. The fluidity of Information gives rise to concerns that it is not reliable because it can be easily corrupted, lost, or accessed by unintended or unauthorized parties.

To avoid easy capture and corruption, Information management must necessarily address the issues of security, integrity, and privacy. Security, integrity, and privacy of Information depend upon reliable control by proper parties over:

1) The channels through which digital information is transmitted,
2) The transmissions themselves,
3) The documents or files transmitted through those channels,
4) The authentication of the cyber identities of Originator(s) sending or receiving those transmissions; and
5) The establishment of ownership, access, storage, retrieval, and use rights in, persistence of content and form, chain of custody, and evidentiary integrity of Information - all of which must be maintained by custodians with no stake in the Information and who operate with a maximum of independence and a minimum of conflicts of interests.

To achieve Informational Privacy, personhood is essential. There must be a person (either an individual, entity, or community) with a claim of ownership in, possession of, or access to the Information in question. Next, there must be property to which ownership is claimed. The digital information must be in some form, such as a pattern of bits or electromagnetic impulses either in transmission or in a fixed medium, that can be cognizable as property, either tangible (like realty or personality) or intangible (like a copyright, trademark, or cause of action). Then there must be a claim of title or right by a person to such property. Usually such a claim is memorialized or fixed in some form so that it may be relied upon and understood in the future.

There must be connected to the property the right of alienation; that is, those with a claim of title or right to the digital information should be entitled in law to assign, convey, or transfer that information, particularly for purposes of access, storage, retrieval, and use. Furthermore, the benefits and burdens of the property must inure only to those with title or right to it so that only the intended parties may enjoy its benefits and assume its burdens. Next, the source or provenance of the Information must be certain. If the source or provenance is not certain, informational accuracy and dependability cannot be assured, thereby creating unmanageable risks and liabilities for those relying upon it. The recipient of such Information must be

guaranteed so that confidential, secret, or sensitive information is not captured or corrupted by unintended parties causing unacceptable levels of risk. Finally, Information must be persistent in both form and content and be impervious to corruption, capture, or alteration during transmission.

These requirements demand that Information be thought of in cyberspace as the analog to real estate in real space. It is not unlikely that in the near future, like real estate, Information will become the subject of life estates, remainders, easements, and even data mining leases, royalties and licenses.

The advent of Information combined with inexpensive and globally available modes of transmission such as the Internet, the World Wide Web, and wireless telecommunication hold out extraordinary promises for the enhancement of both democracy and prosperity throughout the world. The Information Age is, in a very real sense, the next stage of a data revolution – a revolution that began with the invention of moveable type and that has pressed upon the people of the world the need for literacy, communications networks, mutual understanding, tolerance, and cooperation, for global commercial networks dedicated to the generation of greater wealth and better living conditions for greater numbers of people, for a deeper understanding of our human condition through the arts, the sciences, the vocations, and the crafts.

The promising developments of the Information Age, however, must be viewed with circumspection. Though the Information Age presents bright promises of expedience and wealth, it also threatens privacy and personhood as private and personal Information becomes more accessible and easy to exchange.

The issue that must be addressed, and for which the invention (Privacy Architecture™) provides a solution, is how to preserve in cyberspace, at a minimum, the same rights and expectations of privacy security and integrity of information we enjoy in real space.

Cyberspace is a place between the world of the mind and the world of the body. It lies between the world of thought and the world of molecules. Cyberspace is in some way like the world of ideals proposed by Plato; in other ways, it exemplifies the world of Pythagoras -- a world where all things are numbers.

In cyberspace, real world things and real world symbols are represented by zeros and ones. These zeros and ones, in turn, are expressed as electromagnetic impulses or, perhaps more accurately, the presence and absence of electromagnetic impulses in a fixed medium or in transmission.

Cyberspace enables users to manipulate ideas of great complexity with great agility and with a minimum of cost and effort. It frees users from the prison of pen and ink, of time-consuming copying, storing, and searching and retrieving. Cyberspace is the beginning of a world memory. This is as portentous as it is dangerous. The danger lies in the boundlessness of cyberspace. Since cyberspace is essentially a world of fleeting electrons that form a kind of Morse code in which Information is written, cyber boundaries are nothing more than other strings of electrons that identify who owns or has access to the data streams.

Creating boundaries in cyberspace requires the establishment and maintenance of personal identities in cyberspace, specifically, the identities of those persons who own and control given streams of digits. Currently, there are no agreed means for setting those boundaries in a way that will be universally honored. This is not to say that a set of practical approaches is not emerging. Securing and privatizing data is the concern of the here and now. Anyone using computers knows the importance of secure connectivity, firewalls, passwords, encryption, hash algorithms, and the like.

The problem with these solutions is that they provide security, but not privacy. The two are related but distinct, like two sides of a single coin. If security is desired, privacy must usually be sacrificed to get it. The readiest example is that of airport security. Passengers must reveal the private contents of luggage in order to ensure security in air travel. This is the usual way that institutional security is usually obtained, by giving up some measure of personal privacy. By the same token, if privacy is desired, security must usually be sacrificed. Imagine the privacy one could enjoy by being alone and on one's own completely sovereign island. The problem, of course, is that such a solitary citizen of such a tiny country would be vulnerable to being overrun by anyone with a force of two or more. Historically, prisons have been places of high security and little privacy. Convents and monasteries have been places of low security and great privacy.

It is important to remember that in cyberspace, as in real space, security and privacy are rival elements of a paradox. The problem then is how to get the most security for the least sacrifice of privacy.

To answer this question, it is first observed that in cyberspace, privacy is best guaranteed by encryption. However, encryption alone will merely create security by rendering a digital text undecipherable to all but the intended reader. To achieve privacy, the encryption must also somehow encode into the Information the identity of the Originator(s), the identities of those with access to the Information, the date and time of the provenance or transmission of the documents, the chain of custody of the document, and the integrity of the document for purposes of admissibility as evidence in a court of law. Unless the solution attains all these results, as does the invention disclosed herein, true privacy will not be achieved because the reliability of the document, its source, content, persistence, provenance cannot be determined with acceptable certainty. Without such certainty, it cannot be known if the benefits and burdens of the Information in the document will be enjoyed or suffered by the intended parties only rather than by unauthorized or unintended persons.

There are currently two primary choices of encryption, namely, symmetrical one-key encryption and asymmetrical twin-key encryption.

Symmetrical one-key encryption is a coding system – or more accurately, a ciphering system – in which the same key used to encipher a text is also used to decipher it. The key or cipher must be shared between those who encipher and those who decipher a text. Because one-key encryption requires the sharing of the secret cipher or key, it does not work very well in a public messaging system like wireless communication or the Internet. If a sender enciphers a message with a symmetrical cipher, she or he must somehow transmit the cipher to the person who is intended to decrypt the cipher message, which is not practical. Even if the cipher itself were encrypted and sent, the process of sending the cipher would expose it to those who could copy it, analyze it, crack it, and then use it to see things they were not intended to see and possibly create counterfeits or corruptions. Of course, such persons would not let it be known that they had cracked the cipher, so it might be years before the key compromise might be discovered.

The one-key system works well for encrypting Information for storage (so long as the keys are kept in perpetuity), but the one-key system is not good for encrypting Information for transmission.

It is widely held that the best encryption system for the transmission of Information is asymmetrical twin key encryption. This was discovered in 1976 by Whitfield B. Diffie and Martin E. Hellman. Other scientists involved were Rivest, Shamir and Adleman, whose initials RSA are well known in the computer security industry. The system discovered involves mathematical algorithms that produce pairs of numerical ciphers (i.e. twin keys) that are mathematically related. If Information is encrypted with one key, it can be decrypted only with its twin and vice versa. The algorithm that produces these key pairs can produce large quantities of key pairs.

The benefits of twin key encryption are important to the preservation of privacy in the Information Age. Twin key encryption allows one of the keys in the key pair to be a private key, held only by the person generating it. The other key in the pair is the public key and can be made available to the world.

The twin key encryption system has three benefits. First, anyone decrypting the message with someone's public key will know that it had to come from the person possessing the private twin key. Of course, this assumes that the public key was properly certified to that person by reliable authentication procedures at least as dependable as those employed in issuing passports or opening bank accounts. Used this way, the private key becomes a digital signature that can be applied to any Information and verified with its public key in a certificate that contains distinguishing information identifying the holder of the private key. This use of the private key allows the key holder to mark any text with a signature that cannot be copied or used by any other party. If digitally signed Information were to be changed in any way, the change would automatically divorce the digital signature from the Information thus rendering it unsigned.

The second benefit of this encryption system is guaranteed delivery to the intended party. If Information is encrypted with the public key of an intended recipient, only that recipient will be able to decode the Information using his or her private key. This means that the sender can be sure that no other than the intended party can decrypt the Information.

The third benefit of this encryption technology is that the encryption keys work without the need for any key holder to share the secret private key with anyone. This allows each key holder to use the private key without ever exposing it to compromise by having to share it.

Another encryption device used in connection with asymmetrical twin key encryption is the hash number. This number is generated by a mathematical operation performed on the zeros and ones that comprise a digital text. The number derived from this operation is called the "hash." It is a one-of-a-kind number that represents the Information. If a single change of even a single element of the text were made, even if that change amounted only to the closing of a single space between words, then the hash algorithm would produce a different hash number. Before a digitally signed or encrypted message is sent over the Internet or wireless telecommunication systems, the message is hashed, and the hash is sent with the Information. When the Information arrives at its destination, it is hashed again. The two hashes are compared. If they match, then no change occurred in transmission. If they do not match, then there has been a compromise and the receiver/sender is notified of the compromise and may act accordingly. These encryption functions are now carried on fairly seamlessly and in a user-friendly way by the most popular Internet browsers available free on the Internet.

Asymmetrical twin key encryption is not as easy to use as symmetrical encryption, passwords, digital fingerprint identification, retina scans, or other such control methods. But twin keys are better because these other methods are equivalent to a one-key encryption that requires a shared secret. The shared secret is a very dangerous way of encrypting private information. As soon as the secret is shared, it is exposed to compromise. Once compromised, the shared secret can be used to subvert privacy security and integrity of Information. The danger of this is extremely grave to the citizens of an open society.

One of the principal features of the Information Age is the Internet. The Internet started as a military project known as ARPA, which resulted from the linking of computers used by scientific groups, universities, and members of the military industrial complex. Its purpose was to extend and secure communications among members of this group. Eventually, the networks grew into the Internet of today.

Originally, the Internet was funded principally by the U.S. Government mostly through the National Science Foundation. Now the Internet is largely supported by its users. The Internet is not in the control of any particular group. However, prestigious private organizations exert significant influence on the development of the Internet by publishing globally accepted Internet standards, procedures and protocols.

The Internet is at once nowhere and everywhere. The Internet is not a superhighway. It is, perhaps more aptly compared to a cloud composed of and sustained by interrelated communications networks interconnected by telephone lines and satellite systems.

What is currently driving the growth of the Internet is Internet commerce. Internet commerce is the expansion of the Internet from its original use as a passive informational resource to an interactive professional and commercial tool. When it comes to Internet commerce, everything in cyberspace must have its analog in real space. This must be accomplished by means of technological applications that:

1) Recreate in cyberspace the protocols and conditions required in real space for contracting, licensure, the signing and filing of digital documents;

2) Authenticate and certify personal, business, and governmental identities in cyberspace as reliably as they are in real space;

3) Guarantee for cyber citizens at least the same rights they enjoy in the real world venues where they reside;

4) Provide for the creation of non-repudiable, legally-binding digital signatures on digital documents that have the same force, dignity, and evidentiary admissibility as their paper counterparts in the real world;

5) Allow for electronic financial transactions that are as flexible, viable and reliable in cyberspace as in real space; and

6) Provide Informational Privacy.

Cyberspace is possible only because real things and traditional symbols can be expressed as strings of digits of zeros and ones. This is not problematical until human identities are represented in this way. Information that can identify persons, their residences, job, parents, children, addresses, phone numbers – any Information is identifying Information if it than will allow another person to identify, locate, contact,

or make a decision with respect to a given individual. To the extent that identifying Information is not in the control of the person it identifies or of persons with a compelling interest in such Information, that each such person has lost the power of self-determination over his or her past, present, and future. Identifying Information outside the control of the identified person may be altered, corrupted, manipulated, and used in ways that can subvert truth, damage, rob, or mischaracterize the identified person, or do injury to that person's relationships or property. It is critical that ownership and control of identifying Information be maintained by the person whom the Information identifies or such person's authorized designees. To enable this to be done, encryption becomes indispensable. The question is, then, whether one-key or twin-key encryption should be used.

One-key encryption requires that an individual be represented in cyberspace by a cyber ID code consisting of a single number -- a secret that must be shared to be used. Twin-key encryption does not require this. Instead, it involves the use of two mathematically related keys, one private and the other public. This dual representation exactly corresponds to the dual way we identify individuals in the real world. Real people are comprised of both mind and body, both interior and exterior. This dual nature is precisely reflected by the twin key ciphers of the asymmetrical system. The interior is private and represented by the private key. The exterior is public and is represented by the public key. The two keys comprise the single cyber identity of the real world individual. This expression of personhood allows an individual to control his or her own private Information. With the private key, a person can sign a text. This signature establishes putative ownership. Putative ownership is an initial claim of ownership that is rebuttable in a court of law. The private key also fixes the content of the document so that it can not be altered without divorcing the Information from the signature. Also, the use of another person's public key to encrypt Information guarantees that it will be read only by the holder of the corresponding private key. By this means, the signer and owner of Information can bestow rights of access upon others.

In cyberspace, to quote Pythagorus, "all things are numbers." Therefore, Internet security, like everything, consists of zeros and ones and is a matter of binary

encryption codes whose generation, structure, application, and mathematical nature render them (as a practical matter) fail-safe.

In cyberspace, Lincoln's Gettysburg Address, for example is merely an unaesthetic string of zeros and ones. Taken together these digits form a number, the "text number." This number has no meaning with respect to the text. It would be analogous to the sum of all the check numbers in a checkbook -- interesting maybe, but meaningless with respect to the balance on account.

In cyberspace, the Gettysburg Address text number is useful not just because it is made up of all the numbers representing the letters and spaces of the text, but because it can be ignored as such and treated as just a number that can be divided, multiplied, added to, or subtracted from. It can be made a part of a complex formula. In short, it can be transformed by mathematical operations into another binary number whose zeros and ones no longer correspond to the standard accepted codes representing the letters, spaces, and punctuation marks of the original plain text of the Gettysburg Address. In other words, it can be encrypted.

The asymmetrical twin keys are used to encrypt and sign texts. The public and private keys are generated in the user's browser typically by stimulation from a certification authority using an on-line link. During the process of applying for a digital certificate, the certification authority downloads data and instructions to the user's browser, and the public key generated there is, upon authentication, embedded into a usually standardized digital certificate which is then listed in the certification authority's repository where it can be acquired by any party needing it. The user's private key, however, never leaves the browser or the smart card, or token where it was generated. It remains in the user's secure environment.

If Information is encrypted with a user's private key, the Information can only be decrypted with the user's corresponding public key in the user's certificate. If Information is encrypted with the user's public key in the user's certificate (which is publicly available), it can only be decrypted with the corresponding private key in the certificate holder's sole possession. Information may be encrypted more than once and by more than one key.

For example, Information can first be encrypted with the private key of the sender of the Information and then again with the public key of the intended recipient

of the message. By encrypting Information with the sender's private key, it can only be decrypted with the sender's public key in the sender's certificate. When the recipient acquires the sender's certificate and uses the public key in that certificate to decrypt the sender's message, the recipient knows with absolute certainty that the message was signed by the sender. The sender knows that only the recipient can decrypt the message with the intended recipient's private key corresponding to the public key with which it was encrypted.

A user can acquire and maintain a list of certificates belonging both to the user and to others. These certificates can be activated by simple "point and click" procedures.

Referring now to Figure 2A, suppose Alice 60 wants to digitally sign an e-mail message 64 and send it to Bob 62. Alice 60 first composes her message 64, then locates the digital signature icon on her browser, and then clicks on that icon just before sending her message. When she does this, her browser automatically locates Alices's private key A 66 and encrypts her message 64 to Bob 62 with it. When Bob 62 receives the message, his browser automatically seeks out Alice's certificate/public key A 68 and uses it to decrypt the message 64. This protocol assures Bob 62 that the message 64 really came from Alice 60. This assurance is based on the fact that 1) only Alice's private key could have encrypted the message 64, since it was decrypted with public key A 68 and 2) Alice's public key A 66 is embedded in a certificate which has been bound and issued to Alice by a recognized trusted third-party certification authority.

Referring now to Figure 2B, if Alice 60 wants to encrypt her message 70 to Bob 62, she can click on the encryption icon, locate Bob's certificate/public key B 72 in her list of certificates, and use it to encrypt the message (as shown in crosshatch). By encrypting the message 70 with Bob's certificate/public key B 72, Alice 60 is guaranteed that only Bob 62 can decrypt the message 70 with his corresponding private key B 74.

Alice 60 can also sign the message 70 in addition to encrypting it by first clicking on the digital signature icon and then again on the encryption icon before sending the message. In this way the message 70 will be both signed and encrypted,

thereby guaranteeing Alice 60 that the message will be decrypted only be Bob 62, and guaranteeing Bob that the message could have only been encrypted by Alice.

Because of the huge length of these keys (which consist of long, binary numbers), neither key, as a practical matter, can be mathematically derived from its corresponding key or from the algorithm that created them.

Theoretically, no encryption key is unbreakable. Indeed, the National Security Agency of the United States can probably break any currently authorized code in .0002 seconds or less. However, this achievement is extremely expensive. For this reason, no encryption technology available can secure Information transmissions against the resources of a powerful government determined to intercept and compromise it. However, as a practical matter, asymmetrical twin key encryption technology is extremely sound, reliable, and far more secure than the security involved in ordinary Information transmissions and financial transactions.

By using the sender's private key to encrypt a message before sending it, the sender digitally signs Information. This usage of the private number or cipher is called a digital signature. Once a digital document is signed in this way, it is considered a signed document within the meaning of the law authorizing the use an acceptability of digital signatures. This protocol can be used to file legal documents, contracts, and other official papers thereby making the terms, conditions and covenants in Information legally binding so that they cannot later be repudiated by the signer.

Digital certificates can also be used to seal Information and ensure that it cannot be altered even in the slightest degree. This is possible, again, because the text is readable as a binary number. When a message is signed or encrypted, this number is reduced to a hash (or digest), which is a smaller number derived from the text number. The mathematical algorithm used to create the hash number will create a very different hash if just a single digit of the text number is altered. When a signed or encrypted message is transmitted over the Internet, it is accompanied by its hash number or digest. When the transmission is received at its destination, another hash number is generated. The hash number that was sent with the message is then compared to the hash number generated at the destination of the message. If the message has not been tampered with, the two has numbers will be identical. The

slightest tampering (or even unauthorized viewing) of the message will result in a very different hash number at the point of destination. If the hash numbers are not identical, the recipient is warned that the transmission has been tampered with and the transmission may not be decrypted.

4. **Privacy Considerations: Informational Privacy and the Privacy Architecture™**

The invention referred to herein as Privacy Architecture™ has both a technological and a legal component. Technologically, for the purpose of processing, storing, and transmitting Information, the invention employs encryption, particularly asymmetrical twin key encryption, digital certificates, hash numbers, and contemplates the employment of other existing or future security techniques for protecting Information. The invention's organizational legal framework establishes legal and fiduciary duties and structures that assure Informational Privacy. The technological components of the invention alone do not establish Informational Privacy. They must be coupled with the legal components to achieve Information Privacy, which is the end purpose of the invention.

The invention sustains two independent functions. The first is the function of the PKI (public key infrastructure). The second is the function of a PRI (private repository infrastructure).

The PKI function of the invention assures adequate and reliable public key encryption and adequate and reliable management of public keys, digital certificates, and of personal and sensitive Information gathered, used, and maintained as part of public key/digital certificate authentication, issuance and administration. This function is accomplished by the fiduciaries acting within the Privacy Architecture™ under the requirements of the CPS.

The PRI function of the invention assures adequate and reliable management of Information in such repositories. This function is accomplished by the trusts acting within the Privacy Architecture™ under the requirements of the RPS.

Under the CPS, the PKI function is grounded in the Privacy Architecture™ which establishes the PKI as a hierarchy of authorities that together serve to issue secure and reliable encryption keys. These authorities may consist of individuals or entities (trust or private profit seeking or non profit seeking business entities or

government or quasi governmental entities) that may include primary and secondary functions, as approved by the highest ranking authority in the hierarchy of the Privacy Architecture™.

Within the Privacy Architecture™, the highest ranking authority in this hierarchy is the Policy Approval, Control and Management Authority ("PAA"). The PAA oversees the actions of all other members of the public key infrastructure in order to ensure quality control. The PAA controls the quality of digital certificates principally through the publication of the CPS, which requires among other things the issuance of well-formed, reliable, interoperable (i.e., globally acceptable) digital certificates.

Next in the Privacy Architecture's™ PKI are the Issuing Authority, Registration Authority, Authentication Authority, and Services Authority (which may be consolidated in the Certificate Authority ("CA") entity or in one or more other entities). Under the direction of the PAA and bound by the CPS, these authorities oversee the issuing of certificates to users, the registration process, background checks and other authentication protocols, and the maintenance of services related to the uses and applications to which digital certificates can or may be put.

Within this PKI, a CA may issue to a subscriber one or more certificates that certify that this person is the actual person corresponding to the person identified in the certificate.

With respect to an electronic transmission of Information:

1) A transmission is signed when it has been encrypted with the sender's private key, which means that it can only be decrypted by that person's certified public key.

2) A transmission is secured when it has been encrypted with the intended recipient's certified public key, which means that the transmission can be decrypted only by the person possessing the private key corresponding to the intended recipient's certified public key.

3) A transmission is authenticated, that is, delivered precisely as it was sent without alteration of any kind, when the message has been reduced to a hash number that is sent with the message, re-hashed at

the point of destination, and upon comparison the two hashes have been determined to contain no discrepancies.

4) A transmission is transmitted with an expectation of privacy when it has been transmitted under these encryption protocols using the appropriate certificate and certificate extension (these are codes that are issued for specific user functions such as messaging, commercial use, etc.) so as to ensure the highest levels of freedom from invasion of privacy from any individual, person, or entity.

5) A transmission is verified when a valid certification authority has verified the validity of the certificate of the person whose certificate being relied upon has been signed with the certified public key of the certification authority issuing the certificate. This protocol creates a chain of valid certificates that are recognized by the security protocols in the relying party's browser.

Within this PKI a CA may issue one or more types of certificate that can be customized for different uses or can have varying levels of security. For example, a subscriber may purchase only a messaging certificate, based on a declaration of information made by a subscriber under penalty of perjury. Or, it may be authenticated at a higher level by a background check only a social security number, driver's license or student number, and picture ID. For higher levels of authentication for digital certificates, deeper background checks may be required. A subscriber may seek a digital certificate not for an individual but for a server used by a commercial or banking enterprise to receive electronic transmissions of money. Certificates may also be used to limit access to certain web sites, to limit the dollar amounts of transactions, or to avoid the repetitive use of passwords. Restrictions on the use of a certificate are signaled to the relying party in the form of dialogue boxes containing relevant "Warnings" or "Restrictions" or "Limitations ON Warranties" accompanying transmissions of Information. A chart of various levels of certificates based on depth of authentication requirements is shown in Figure 3.

Further security can be achieved in PKI management for different digital certificates by (1) additional CPS protocols controlling the digital certificate authentication process, including certificate renewals, suspensions, and revocations,

(2) the use of biometric security devices (voice prints, fingerprints, etc.), (3) the implementation of serial messaging, (4) the placement of limitations on the content of value of transmissions, and (5) the acquisition of traditional bonds or letters of credit.

Digital certificates ensure that commercial protocols in cyberspace are at least as reliable as they are in real space and that Internet transmission of Information be at least as secure as conventional communications.

In summary, the hash algorithms render the messaging tamper-proof in transmission and the asymmetrical twin-keys can establish reliable cyber identities and, consequently, putative rights of ownership, access, possession, processing, use and alienation of Information.

Nevertheless, even in combination these technologies alone cannot deliver Informational Privacy until they are combined with the organizational and legal benefits that together compromise the invention Privacy Architecture™ disclosed herein.

Prior to the invention, what has been missing, and what is now provided by the invention, are systems and methods: (1) for reliably authenticating the identities of real world persons, certifying those identities, and binding them to public keys, and reliably preserving signed and/or encrypted documents in a way that establishes, preserves, and protects ownership rights, access rights, benefits and burdens, provenance, persistence and integrity of both form and content, chain of custody, and evidentiary admissibility over undetermined periods of time so the Information may be relied upon as legally-binding and legally enforceable not only in the here and now, but in the near and distant future as well; and (2) for preserving for the Information Originator(s) control of personal and sensitive Information under fair information practices that are assured by unbiased legal and/or fiduciary custodians. The charts showing the benefits of the invention with respect to PKI and PRI are attached as Appendix A, which is not intended to be exhaustive of the benefits that may arise from the invention, nor do all of the benefits of the invention need to be present in any particular embodiment of the invention, which is defined by the claims rather than Appendix A.

When the Privacy Architecture™ is used to preserve the original content of Information, both the original form of the Information and the data that was originally

contained in the Information are typically preserved. However, the term "preserving the original content" of Information, as used in the claims, refers to preserving either the original form of the Information, the data that was originally contained in the Information, or both.

5. **Exemplary Organizational and Legal Environment**

Within the meaning of this document, a PKI is a hierarchy of authorities that cooperate to provide, secure, and administer asymmetrical twin key, triple key, or other multiple key encryption (e.g. digital certificates, digital signatures) as well as digital repositories of keys and data, and digital-certificate-based applications), according to policies, procedures, protocols, and procedures as well as private, national and international standards that ensure high-level security for analog or digital transmissions and that preserve end-user Informational Privacy and property rights.

Within the meaning of this document, a PRI is a hierarchy of authorities that cooperate to provide Informational Privacy with respect to Information reposed in repositories operated by neutral third party custodies requiring compliance with fair information practices.

According to the present invention, a novel PKI/PRI is organized in the form of the Privacy Architecture™. This PKI/PRI can be designated as a legal, or fiduciary-based, or trust-based PKI/PRI. Such a PKI/PRI performs the functions described herein and relies upon, involves, or makes use of at least one business entity and at least one trust, business trust, non-profit corporation, other fiduciary entity, or other entity exercising a protective standard of care approaching that of a fiduciary (hereinafter jointly and severally referred to as "trust"). The fiduciary-based PKI can be used to perform novel methods of maintaining Public Key Management and Informational Privacy in information whether collected, created, used transmitted, stored, or processed.

Referring now to Figure 4, Legal and/or Fiduciary-Based PKI/PRI 100 (hereinafter "FB PKI/PRI") is an alliance or affiliation of entities that provides Internet privacy and security solutions in the form of PKI/PRI consultation, digital certificates, digital signatures, repositories, and secured document management

cyber identities and digital certificates for FB PKIs/PRIs and users 104 and their clients and relying parties.

FB PKI/PRI 100 and PSA 102 employ any desired type of encryption, data processing, and repository solutions to give users 104 the efficiency of the Internet with more security than is available in traditional paper processes. This combination of legal or fiduciary duties and technology protects the privacy of users 104. This protection is particularly important to lawyers, doctors, accountants, therapists, and others because FB PKI/PRI 100 and PSA 102 protect these professionals with the same high level of care they owe to their own clients. As used herein, the term "duty of confidentiality for sensitive information" refers to this high level of care or a similar duty of confidentiality.

As part of FB PKI/PRI 100, fiduciary network 106 includes PSA 102 and two non-business trusts. The constituent members of this example of a fiduciary-based PKI/PRI 100 are:

Primary Servicing Authority (PSA) 102, a for-profit entity in the form, for example, of a "C" corporation;

Certification Authority/Repository (CAR) 112, a non-profit corporation;

CA Trust 114, a legally settled trust;

Policy Approval Authority (PAA) 110, a non-profit corporation;

Data Trust 108, a legally settled trust; and

Network LLC 106, a limited liability company comprising PSA 102, CAR 112, and PAA 110.

FB PKI/PRI 100 achieves public key management and Information Privacy by using legal or fiduciary entities (trusts or their functional equivalents) to insure:

1) The reduction of conflicts of interests among those with control over public key and Information;

2) The separation of security and control functions among several parties thereby enhancing security protections of both PKI and PRI functions;

3) The placement of the administration of public keys and Information in the hands of trustee or protecting entities who cannot profit from security breaches or privacy invasions;

4) Means for customers to transfer to a trust corpus, under the legal or fiduciary custodianship of a third-party trustee or protecting entity, the customers' identified and marked Information and public keys as the private property of Originators or digital certificate customers;

5) Means for customers to express clearly and provide evidence of their expectations of privacy in Information whether collected, created transmitted, stored, processed, or used; and

6) Means for customers to retain control of Information while enjoying Informational Privacy protections offered by legal or fiduciary entities with expertise in the arena of Information security, integrity, encryption, Information Privacy and Information management.

Though all financial interest in Network LLC 106 is held solely by PSA 102, the management of the Network 106 for security and privacy purposes rests with the trustees of the non-profit trusts, the duty of which trustees is to securely manage the public keys and to preserve the rights of privacy of customers in Information. As noted previously, the non-profit trusts are Data Trust 108 and CA Trust 114, while the trustees of these trusts are, respectively, PAA 110 and CAR 112.

The mere existence of legal or fiduciary duties with respect to the property of others, whether Information, money, copyrights, patents, etc., is insufficient to protect such property and, specifically, to assure Informational Privacy or secure public key management. Conflicts of interest will exist if a fiduciary has control over a beneficiary, has adverse interests to those of a beneficiary, is not disinterested, is not evenhanded, is not neutral, has actual or probable claims against a beneficiary arising outside the protector-beneficiary or fiduciary-beneficiary relationship, has unauthorized access to confidential information with respect to the beneficiary, advises the beneficiary in other matters, has an economic interest that conflicts or is likely to conflict with that of a beneficiary, is dependent on a beneficiary for other than fiduciary fees, or maintains an interest that could conflict with the duty to protect a beneficiary's property interests. Moreover, a fiduciary should be licensed, regulated, audited, subject to review; and the fiduciary's action should be disclosed with notice to beneficiaries, giving them due process, specifically an opportunity to

object and be heard. Only with these safeguards can a legal protector or fiduciary be truly unbiased and can act without conflicts of interest.

In this embodiment of the invention (the Privacy Architecture™), the legal protector or fiduciary of CA Trust 114 and the fiduciary of the Data Trust 108:

1) Have neither control nor do they exercise control over any beneficiary or party protected by a trust;
2) Hold no interest adverse to such beneficiary;
3) Are disinterested, even-handed, neutral, unprejudiced, and without an actual or probable claim against a beneficiary;
4) Have no unauthorized access to Information of the beneficiary;
5) Are not adverse to a beneficiary in the matters outside the fiduciary-beneficiary relationship;
6) Have no economic interest that actually conflicts or probably could conflict with that of a beneficiary;
7) Are not dependent upon a beneficiary for other than fiduciary fees;
8) Maintain no duty that could conflict with the fiduciary duty to protect the interests of a beneficiary in a trust corpus or as otherwise defined in the fiduciary beneficiary relationship; and
9) Are regulated, licensed, audited and subject to review under rules that require notice of such actions to beneficiaries.

The following description relates to the roles and duties of the various entities in Figure 4 according to this embodiment of the invention.

Data Trust 108 serves to safeguard the Information of users 104 (e.g., customers, subscribers, and licensees) of FB PKI/PRI 100.

PAA 110 is a non-profit corporation that serves as the trustee of Data Trust 108. It also serves as the PAA of FB PKI/PRI 100. As such, PAA 110 is responsible for creating, maintaining, promulgating, and auditing the public key management and Informational Privacy policies, procedures, protocols, and practices embodied in the CPS and RPS that protect the beneficiaries public keys and Information for both user 104 and relying parties. These policies, procedures, protocols, and Practices of both CPS and RPS are manifested in contracts, licenses, warranties, limitations on warranties, and in certification practices statements. Neither the Data Trust 108 nor

the trustees of the Data Trust 108 implements the standards in the CPS and RPS. Implementation is the duty of the CA Trust 114.

CA Trust 114 safeguards the encryption and repository technologies used by FB PKI/PRI 100 to enable privacy and provide security with respect to both Information and public key management.

CAR 112 is a non-profit corporation that serves as the trustee of CA Trust 114. CAR 112 also serves FB PKI/PRI 100 as its governmentally-licensed certification authority and recognized repository responsible for assuring the secure generation, issuance, certification, and administration of the asymmetrical encryption ciphers that provide the security and integrity that underlie the Informational Privacy protections afforded to users 104 and licensees. Both as trustee of CA Trust 114 and as the FB PKI/PRI 100 certification authority and recognized repository, CAR 112 implements the public key management and Informational Privacy policies, procedures, protocols, and practices promulgated and issued as CPS and RPS and other mandates and audited by PAA 110 in its role as PAA of the network.

PSA 102 is the profit-making entity with FB PKI/PRI 100. It owns the financial interest in FB PKI/PRI 100 as well as any intellectual property, applications, and privacy and security enabling products. This company provides many of the registration, documentation, authentication, validation, and related services required by FB PKI/PRI 100. Because the trusts 108 and 114 assume the duty of protecting end users' privacy and security and safeguarding encryption and repository technology against compromise or abuse, PSA 102 is free to pursue its profit-making interests without conflict. PSA 102 can be, for example, a "C" corporation.

Other members, partners, strategic allies, customers, and customer representatives may participate in this legal or fiduciary-based PKI/PRI. Moreover, the specific structure of FB PKI/PRI 100 can differ from that illustrated in Fig. 4 so long as there exist one or more trusts for protecting the privacy and security of Information and assuring secure public key management for users 104 and for safeguarding physical security and privacy tools 116 (e.g. data encryption and repositories) against abuse, and so long as there also exists a profit-making entity that is free from conflicts of interest and does not have the fiduciary duties of trust/fiduciary entities.

The entities within the Privacy Architecture™, including both its PKI/PRI functions, can work together as demonstrated the following illustration. When PSA 102 sells a digital certificate, it does so pursuant to an operating agreement FB PKI/PRI 100 as well as a strategic alliance contract among the members of Network LLC 106. Under the terms of these agreements, when user 104 applies for a digital certificate 118, as shown in Figure 5, PSA 102 sells and supplies the certificate to the user. This transaction involves the issuance of a public and private key pair as well as a digital certificate 118 in which the public key 122 is embedded. Under the Privacy Architecture™ illustrated by FB PKI/PRI 100, at the time of sale the title to the key pair is established as follows:

The generation of private key 120 takes place transparently in the user's Internet browser or on a smart card or token. Upon its sale, legal and equitable title and unfettered possessory interest in this private key vests with the end user as shown at reference number 132.

The generation of public key 122 takes place transparently in the user's Internet browser or on a smart card or token along with the generation of the private key 120. However, upon its sale, the equitable title in the public key 122, the digital certificate 118, and the personal identifying documents and information ("PID") used to authenticate the identity of the subscriber vest with the end user as shown at reference number 134, while legal title to the public key, the digital certificate, and the PID pass to Data Trust 108 by virtue of the contract between PSA 102 and the user 104 as shown at reference number 136. This legal transfer is made pursuant to policies, procedures, and protocols set forth in the CPS required by the terms of a Declaration of Trust of Data Trust 108. The purpose of this transfer of legal title is to provide the Data Trust 108 with legal title and full authority to provide secure public key management, safeguard the Informational Privacy to any personal or sensitive Information, enhance the expectation of privacy of the end user in such Information, and enhance the security of the FB PKI/PRI 100 by fully empowering the trustee, PAA 110 to ensure that public keys, digital certificates, and the PID are used in accordance with the CPS and RPS of the PKI/PRI.

PAA 110 is responsible for establishing the overall policies, procedures protocols, and practices by which the titles are transferred, the public keys securely

managed, and the Informational Privacy or Originators, customers and relying parties are protected in the trust corpus and repositories. CAR 112 is responsible for implementing the policies, procedures, protocols, and practices governing all aspects of secure public key management under the CPS and Informational Privacy under the RPS.

This Privacy Architecture™ as embodied in the FB PKI/PRI 100 mitigates conflicts of interest through the separation of security and fiduciary duties among the UTN entities comprising the Privacy Architecture™. It also creates a scalable and secure legal and business framework that allows for the creation of multiple PAAs, CAs, repositories, and profit-making entities either jointly, as subordinates, in a hierarchy, or as performing secondary functions. It also protects users' cyber identities, private/confidential Information, and the interests and rights of other parties. It inherently addresses the security, integrity, Informational Privacy, and trust needs of e-commerce business-to-business (B2B) market participants. Through this novel Privacy Architecture™, FB PKI/PRI 100 provides real Informational Privacy through real trusts in a virtual world.

FB PKI/PRI 100 separates its security functions among three entities to avoid certain conflicts of interest and to mitigate others, thus lessening the potential for security breaches and privacy invasions. Within FB PKI/PRI 100, the functions of making security policies and protecting the privacy of end users does not rest with the profit-making entity. This prevents the profit-motive from eroding and unduly influencing security policies that must be maintained at the highest levels for users' Informational Privacy and security. Encryption technology and certification procedures are separated from the profit-making entity as well. This prevents the profit-motive from subverting key and management and certification engine malfeasance or misfeasance.

The Privacy Architecture™ leaves the profit-making and business functions to be carried on by PSA 102. The Board of Directors, President/CEO, and management team of PSA 102 are not burdened with conflicting duties with respect to security and privacy protection of users 104 or of certification licensing and encryption technology administration. The management of PSA 102 is free to pursue the single fiduciary responsibility of increasing its value for shareholders. This multi-layered structure

allows the CPS and RPS to be established by one entity, to be implemented by another entity, and exploited for profit by a third entity. By mitigating and creating checks and balances on conflicts of interest, privacy, security, and integrity in public keys and Information is enhanced and strengthened and potential compromise are lessened.

The Privacy Architecture™ embodied, for example, in FB PKI/PRI 100 of Figure 4, with Informational Privacy, provides at least the following benefits with respect to the transmission, storage, access, retrieval, use, and processing of Information:

1) Independent unbiased fiduciary oversight over Information management processes;
2) Privacy law compliance, particularly for multinational companies required to comply with privacy laws of foreign jurisdictions;
3) Clarification of ownership rights to and expectations of privacy in personal and sensitive Information;
4) Restricted and protected access to such Information;
5) User control of Information to ensure review, correction, and traceability;
6) Liability and risk management and reduction for data managers;
7) Compliance reviews to ensure adherence to fair information and secure digital certification practices;
8) Preservation of Information integrity, including:
    a) Non-repudiation of digital signatures and digital Information
    b) Evidentiary integrity
    c) Chain of custody
    d) Persistence of form and content
    e) Verification of claimed ownership rights or access rights
    f) Date and time stamping; and
    g) Access and retrieval registry;
9) Protection against technological advancements and obsolescence;
10) Uniform fair information policies, procedures, and practices that:

a) Establish obligations and responsibilities for personal and sensitive Information,

b) Maintain transparent processing systems,

c) Create special protections for sensitive Information, and

d) Enforce effective oversight of the uniform and unbiased treatment of personal and sensitive Information.

The Privacy Architecture™ can also preserve intellectual property interests of users 104. When FB PKI/PRI 100 licenses a repository service or digital certificate product to a user 104, pursuant to a licensing contract, legal title to the digital certificate or Information reposed in the Privacy Architect repository vests in Data Trust 108, while equitable title vests in the user 104. The user 104 is free to use the digital certificate or Informational pursuant to the license, but may not violate provisions of either the CPS or RPS. If any such provisions is violated, Data Trust 108, as the holder of the legal title to the users digital certificate license, may require the revocation or suspension of that license by CAR 112 under the FB PKI 100 operating agreement. The revocation or suspension is implemented by CAR 112 as the licensed CA rather than by the profit-making entity. This avoids a conflict between the need to revoke a license to preserve security or Informational Privacy and the need to preserve the goodwill of a customer opposing such a revocation and possibly even threatening litigation. This Privacy Architecture™ places the revocation or suspension decision beyond the profit making entity PSA 102, thus protecting that entity's assets.

With respect to the asymmetrical twin key pairs issued under the Privacy Architecture PKI by which a user 104 may sign or encrypt Information, the Privacy Architecture of Figure 4 enhances the reliability of public keys by placing the duty to ensure acceptable levels of registration, authentication, and certification of digital certificates in the hands of a party separate from the marketing and selling agenda of those digital certificates, CAR 112. As trustee of CA Trust 114, CAR 112 has legal title to the encryption technologies and the power to prevent their compromise or abuse by PSA 102. The trustees, PAA 110 and CAR 112, can even-handedly enforce security and privacy policies and procedures for the provision, preservation, and protection of PIDI and other personal or sensitive Information pursuant to the PKI

CPS or the PKI RPS. PAA 110 oversees the administration, revocation, suspension, reinstatement, and renewal of digital certificates by CAR 112 as part of the PKI function and oversees Information Privacy protections and repository operations as part of the PRI functions. In other words, the policies, procedures, protocols, and practices promulgated by one trustee are implemented by the other trustee so that maximum privacy and maximum security are preserved. This statement is not intended to limit or fix the trust configurations the invention may assume.

The Privacy Architecture™ also prevents the profit making entity, PSA 102, from subverting the security of the structure for profit. In a hostile take-over or in an acquisition, ownership of the profit-making entity may change. With such a change may come a new board that may see more value in subverting privacy, security and integrity of public keys and Information than in maintaining them. The Privacy Architecture™ provides two independent trustees, PAA 110 and CAR 112, to block any illegal or subversive use of encryption or repository technology by the PSA 102 or any successor in interest. Neither the trustees PAA 110 and CAR 112 nor the trusts, Data Trust 108 and CA Trust 114, have any authority to interfere with the legitimate business of the profit making entity. This benefit can be used as a marketing feature. The trusts and trustees create a legal firewall around the encryption and repository technology upon which the profit-making entity relies, thus strengthening the value of the marketable solutions that are predicated on those technologies. This is also, an added value to investors, who presumably would prefer to invest in a company that can offer more value to its customers because its security and privacy systems cannot easily be compromised or subverted by changes in structure, ownership, or management.

The Privacy Architecture™ also allows the user 104 of FB PKI 100 to repose Information with Data Trust 108, as a trusted third-party. By doing this, a user can retain all of the beneficial interests and use of the Information, while storing it under legal and technological protocols that provide or enhance Informational Privacy create or enhance an expectation of privacy and privacy rights, thus rendering them more likely to be honored by courts. The result is not only a repository in the technical sense, but in a legal sense of a trust corpus that protects Information not only from

theft but from invasions of privacy, and from unwanted liabilities and risks stemming from the unnecessary management of the personal or sensitive Information of others.

Trusts work better to inspire confidence than contracts to provide maximum privacy with maximum security either with respect to PKI or PRI functions of the Privacy Architecture. This is so because trusts create in trustees legally enforceable fiduciaries duties, including the duty of loyalty to trust beneficiaries, while contracts merely impose liabilities on the parties. But this statement is not meant to limit the trust or legal configurations the invention may assume.

Under a trust, a user 104 is a beneficiary with clearly delineated rights that must be protected by the trustees who have no other duty and no conflicts of interests and must act with loyalty to the beneficiary. In contrast, a customer who is only a party to a contract may also be "protected," but the protection is limited to good faith and fair dealing on the part of other contracting parties. The standard of good faith and fair dealing is a lesser standard than that of fiduciary responsibility. Unlike a fiduciary, parties to a contract are not prohibited from acting upon conflicting interests or interpreting or implementing contract provisions in ways that are disloyal to the customer or biased in favor of other parties, yet still technically within the requirement of good faith and fair dealing.

The Privacy Architecture™ illustrated in Figure 4 allows businesses required to provide customers with higher standards of care or with fiduciary duties to go on-line without compromising these higher standards. When it comes to privacy and security in Information management, FB PKI/PRI 100 affords professionals including lawyers, accountants, doctors, therapists, etc., the same high standards of care and fiduciary duty that these professionals are required to provide to their clients, patients, and customers in the management of their confidential and secret information.

Trusts also require trustees to safeguard property for beneficiaries. Under the Privacy Architecture™, restricted and unrestricted rights of ownership and access to Information can be established with clarity and sustained over time because they are submitted with the Information to the custodianship of a trusted third-party fiduciary.

The Privacy Architecture™ and the associated methods of transmitting, storing, and processing Information as a part of its PKI and PRI functions ensure that the identified signer is the Originator of the digitally signed Information. It also

ensures that only the intended recipient(s) can read the Information and that the Information cannot be tampered with or even read during transmission without an alert being sent to the sender and intended recipient. The Privacy Architecture™ PKI and PRI functions also ensure that the party or parties digitally signing Information will be legally bound by the obligations set forth in the Information to the fullest extent of the law and that the Information is date-stamped, time-stamped, enrolled, and preserved in trust in a repository for the benefit of its owners and those with access rights.

The Privacy Architecture™ disclosed herein is flexible so that it can be adapted to include additional policy approval authorities, certification authorities/repositories, and primary servicing authorities. Figure 6 illustrates one example of a fiduciary network 206 that has a plurality of certification authorities/repositories (CAR) 112a-112d and a plurality of primary servicing authorities (PSA) 102a-102d. Fiduciary network 216 is part of a fiduciary-based public key infrastructure and private repository infrastructure that is similar to FB PKI/PRI 100 of Figure 4, with the exception that fiduciary network 216 has a plurality of CARs 112a-112d and PSAs 102a-102d.

The multiple CARs 112a-112d and PSAs 102a-102d can be established to serve different geographical regions, different industries, or otherwise as desired. Each CAR 112a-112d is a trustee of a corresponding trust (not shown), which is similar to CA Trust 114 of Figure 4. Moreover policy approval authority is a trustee of a trust (not shown), which is similar to Data Trust 108 of Figure 4.

In Figure 6, each CAR 112a-112d operates in conjunction with the same policy approval authority (PAA) 110. In other networks, each CAR 112 could operate in conjunction with a different PAA or with more than one PAA, depending on the operating agreement used in fiduciary network 216.

6. Examples of the Implementation Full Informational Privacy

The Privacy Architecture™ of Figure 4 enables parties to use the Internet and wireless communications to create digital and electronic contracts that are as trustworthy as their traditional paper counterparts. Figure 4 illustrates users 104 reposing Information in a physical repository 119, which is a physical storage device or medium protected by physical security and privacy tools 116. The physical

security and privacy tools 116 can be the data encryption, hash numbers, or other technological processes or mechanisms that are established under the security policies established by PAA 110 and implemented by CAR 112.

FB PKI/PRI 100 allows e-contracting parties and relying parties to repose legally binding digital and electronic documents in secure, private repositories, managed by neutral third-party protecting or fiduciary custodians under protocols that preserve such documents reliability and legal integrity over indefinite periods of time. As a result, users can bring numerous paper processes on-line with confidence in their privacy, security, and integrity. Users who are associated with a contract processed according to the invention can be the contracting parties, the beneficiaries of the contract, parties relying on the contract or parties that have some other relationship with the contract. The paper processes that can be brought on-line can include letter of credit transactions, loan applications, commercial and residential real estate closings, the on-line development of intellectual work products, communications among clients and their lawyers, accountants, doctors, therapists, and other professional charged with keeping client confidences and secrets.

In addition to e-contract data vaulting, the Privacy Architecture™ can secure and preserve Informational Privacy in electronic transmissions among companies, subsidiaries and partners of trade secrets, pricing lists, marketing strategies, while providing a mechanism to vault and track confidential materials. It can further allow application service providers (ASPs) to defer the risks and liabilities of personal, sensitive, and confidential Informational management to Information Originators, digital signatories through the fiduciary custodians within the invention. The Privacy Architecture™ can also provide a legal and technological framework for the creation and preservation of Informational Privacy in personal or sensitive medical records while reducing the risks and liabilities of health care professionals currently burdened with the possession and management of this Information. It can provide a secure means to ensure Informational Privacy in the collection creation, transmission storage, processing or use of personal or sensitive Information of students and teachers at all educational levels, while clarifying and protecting the rights of students, faculty, colleges and universities in intellectual property of all kinds.

The present invention referred to throughout as Privacy Architecture™, together with PKI and/or PRI function, may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed is:

1. In an organizational structure that includes an affiliation of entities, a method of storing Information in a repository, with a fiduciary duty being owed to a user associated with the Information such that the Information is secured, the method comprising the acts of:

obtaining Information from a user;

storing the Information in a repository operated by one or more of the entities in the affiliation of entities, wherein the entities include at least a first trustee of a first trust and a for-profit entity that operate together to secure the Information; and

while the Information is stored in the repository, securing the Information using security policies established by the first trustee, the user being a beneficiary of a fiduciary duty of at least one trustee included in the affiliation of entities.

2. A method as recited in claim 1, wherein the Information stored in the repository constitutes the res of a corpus of at least one trust.

3. A method as recited in claim 1, wherein the security policies and the fiduciary duty preserve the original content of the Information.

4. A method as recited in claim 3, wherein the security policies and the fiduciary duty preserve the original content to the extent that the Information stored in the repository can serve as evidence of the original content in a court of law.

5. A method as recited in claim 1, wherein the security policies and the fiduciary duty preserve confidentiality of the Information and prevent unauthorized disclosure of the Information.

6. A method as recited in claim 5, wherein the security policies and the fiduciary duty preserve confidentiality to at least the degree that is associated with a professional duty of confidentiality for sensitive Information.

7. A method as recited in claim 1, wherein the security policies and the fiduciary duty establish fair information practices with respect to the Information.

8. A method as recited in claim 7, wherein:

the affiliation of entities operates in a first country;

the user is an entity that operates in the first country and also in a second country that requires the entity to store Information only in countries that have fair information practices; and

the fair information practices established by the security policies and the fiduciary duty are sufficient to satisfy the requirement of the second country that the entity store Information only in countries that have fair information practices.

9. A method as recited in claim 1, wherein:

the entities further include a second trustee of a second trust, the second trustee being responsible for implementing the security policies; and

the Information is secured as the second trustee implements the security policies.

10. A method as recited in claim 9, wherein the first trustee and the second trustee are non-profit entities.

11. A method as recited in claim 9, wherein the first trustee, the second trustee and the for-profit entity operate under an operation agreement that provides that at least one of the first trustee and the second trustee can prevent the for-profit entity from engaging in practices that would violate the security policies.

12. A method as recited in claim 1, further comprising the acts of:

at least one trustee issuing a digital certificate and an associated public key and private key pair to the user, such that:

the user, at the discretion of said at least one trustee, receives both legal and equitable title to the private key and only equitable title to the public key and the digital certificate; and

said at least one trust receives legal title to the public key and the digital certificate.

13. In an organizational structure that includes an affiliation of entities, including at least a first trustee of a first trust and a for-profit entity, a method of establishing security policies to be practiced by the affiliation such that Information can be stored in a repository with a fiduciary duty being owed to a user associated with the Information, the method comprising the acts of:

establishing security policies by the first trustee that are to be implemented such that the affiliation of entities can:

obtain Information from a user;

store the Information in a repository established by one or more of the entities in the affiliation of entities; and

while the Information is stored in the repository, secure the Information using said security policies, the user being a beneficiary of a fiduciary duty of at least one trustee included in the affiliation of entities such that the user can be assured that the Information is secured.

14. A method as recited in claim 13, wherein the first trustee operates as a policy approval authority and the security policies are established by a CPS.

15. A method as recited in claim 13, wherein the Information stored in the repository constitutes the res of a corpus of at least one trust.

16. A method as recited in claim 13, wherein the security policies and the fiduciary duty preserve the original content of the Information.

17. A method as recited in claim 13, wherein the security policies and the fiduciary duty preserve confidentiality of the Information and prevent unauthorized disclosure of the Information.

18. A method as recited in claim 13, wherein:

the entities further include a second trustee of a second trust, the second trustee being responsible for implementing the security policies; and

the Information is secured as the second trustee implements the security policies.

19. In an organizational structure that includes an affiliation of entities, including at least a first trustee of a first trust and a for-profit entity, a method for the first trustee to implement security policies such that Information can be stored in a repository with a fiduciary duty being owed to a user associated with the Information, the method comprising the act of:

issuing, by the first trustee, a digital certificate to the user, the user receiving legal and equitable title to a private key associated with the digital certificate and equitable title to the digital certificate and to a public key

associated with the digital certificate, the first trust receiving legal title to the digital certificate and to the public key, such that the affiliation of entities can:

obtain Information from a user, the Information including a digital signature created by using the private key;

store the Information in a repository established by one or more of the entities in the affiliation of entities; and

while the Information is stored in the repository, secure the Information using said security policies, the user being a beneficiary of a fiduciary duty of at least one trustee included in the affiliation of entities such that the user can be assured that the Information is secured.

20. A method as recited in claim 19, wherein the first trustee is a non-profit entity.

21. A method as recited in claim 19, wherein the first trustee operates the repository and is responsible, within the affiliation of entities, for performing the acts of:

obtaining the Information from the user; and

storing the Information in the repository.

22. A method as recited in claim 19, wherein the security policies and the fiduciary duty preserve the original content of the Information.

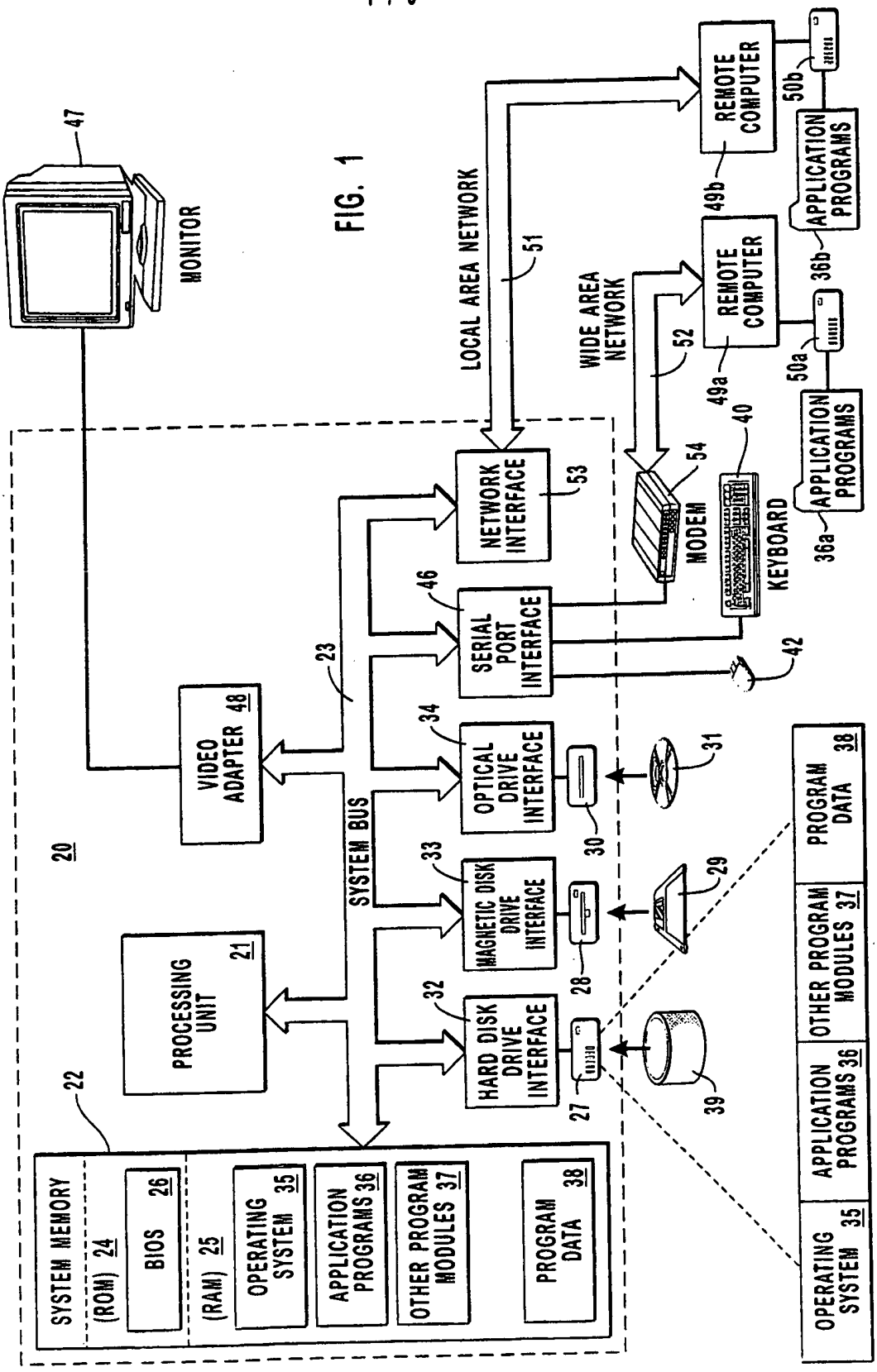
23. A method as recited in claim 19, wherein the security policies and the fiduciary duty preserve confidentiality of the Information and prevent unauthorized disclosure of the Information.

24. A method as recited in claim 19, wherein:

the one or more trustees further includes a second trustee; and

the security policies implemented by the first trustee have been established by the second trustee.

25. In an organizational structure that includes an affiliation of entities, a method of preserving the original content of Information stored in a repository, with a fiduciary duty being owed to a user associated with the Information such that the user is assured that the original content is preserved, the method comprising the acts of:


47
MONITOR
FIG. 1
LOCAL AREA NETWORK
51
WIDE AREA NETWORK
52
REMOTE COMPUTER
49b
50b
APPLICATION PROGRAMS
REMOTE COMPUTER
49a
50a
36b
APPLICATION PROGRAMS
36a
40
KEYBOARD
54
MODEM
NETWORK INTERFACE
53
46
SERIAL PORT INTERFACE
42
23
VIDEO ADAPTER 48
34
OPTICAL DRIVE INTERFACE
31
30
SYSTEM BUS
33
MAGNETIC DISK DRIVE INTERFACE
29
28
20
PROCESSING UNIT
21
32
HARD DISK DRIVE INTERFACE
27
39
22
SYSTEM MEMORY
(ROM) 24
BIOS 26
(RAM) 25
OPERATING SYSTEM 35
APPLICATION PROGRAMS 36
OTHER PROGRAM MODULES 37
PROGRAM DATA 38
OPERATING SYSTEM 35
APPLICATION PROGRAMS 36
OTHER PROGRAM MODULES 37
PROGRAM DATA 38

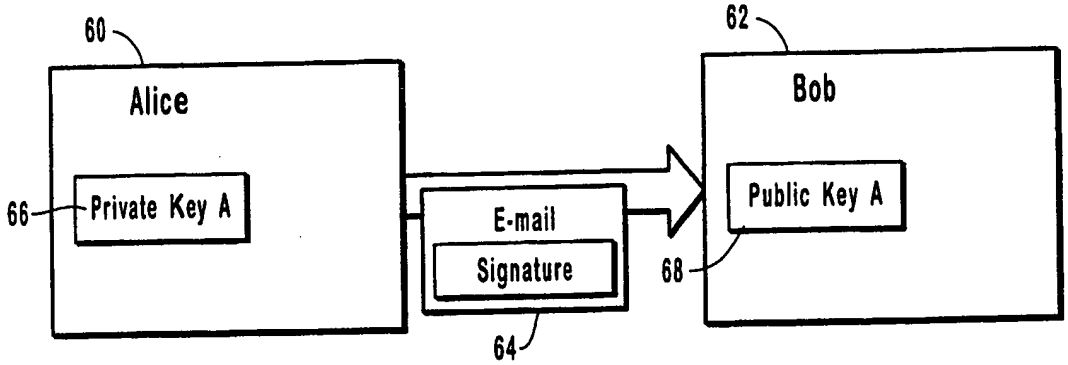

60
Alice
66
Private Key A
E-mail
Signature
64
62
Bob
Public Key A
68

FIG. 2A

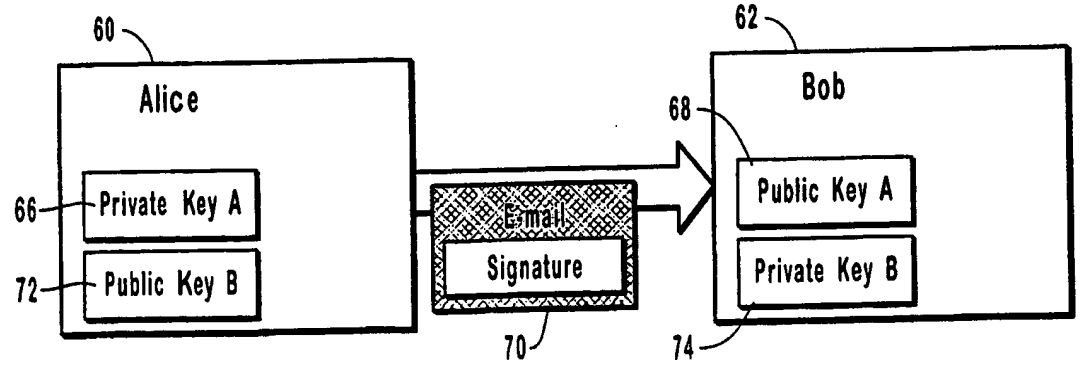

60
Alice
66
Private Key A
72
Public Key B
E-mail
Signature
70
62
Bob
68
Public Key A
Private Key B
74

FIG. 2B

Digital Certificates

Type of Certificate	Purpose of Certificate	Type of Authentication	Comments
Access Certificate with no background check	Used for persistence of identification within a process that will have an eventual face-to-face verification	• Verification of e-mail address • No background check • Assumed eventual face-to-face verification	• Used to establish persistence of ID
Access Certificate with on-line background check and face-to-face verification	For processes that will have an eventual face-to-face verification but require an upfront on-line identification for tying ID to historical information	• Uses an on-line background check of "wallet data" • Assumed eventual face-to-face verification	• Weeds out fakes
Access Certificate with a robust, on-line background check but no face-to-face verification	For processes that are satisfied with a more powerful on-line background check	• Uses a robust on-line background check of detailed personal data • Possible out-of-band transmission of initiation password	• Should be presented as a legally-binding certificate alternative
Certificates with verification conducted by a fiduciary-certified RA	When company or organization wants to conduct their own authentication	• RA specifies authentication criteria • RA conducts authentication process	• Certificates will have any authority RA wants to grant
Legally binding certificate with legal document-signing capabilities	For those markets or customers who require a strong, face-to-face verification due to level of authority in certificate	• Requires ether face-to-face verification or a notarized physical form of documentation	• Options-credit check and/or criminal background check • Can include biometric verification
Legally binding certificate with special rights (professional designation, no criminal record, etc.)	For those markets or customers where certificate will give rights above and beyond identification or legal document-signing capabilities	• Requires either a face-to-face verification or a notarized physical form of documentation • May require notarized proof of special designation	

FIG. 3

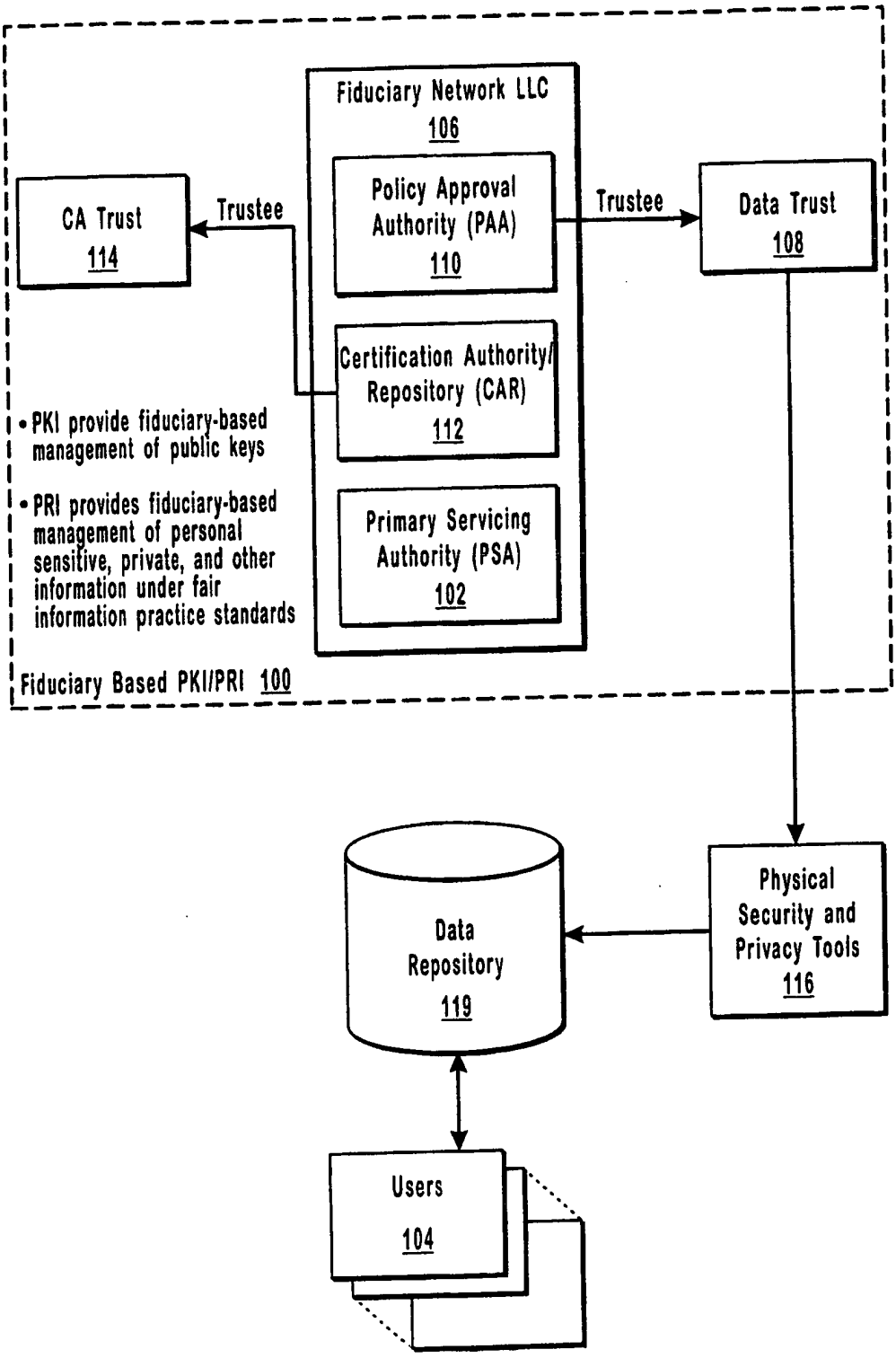

Fiduciary Network LLC
106
CA Trust
114
Trustee
Policy Approval Authority (PAA)
110
Trustee
Data Trust
108
Certification Authority/ Repository (CAR)
112
• PKI provide fiduciary-based management of public keys
• PRI provides fiduciary-based management of personal sensitive, private, and other information under fair information practice standards
Primary Servicing Authority (PSA)
102
Fiduciary Based PKI/PRI 100
Data Repository
119
Physical Security and Privacy Tools
116
Users
104

FIG. 4

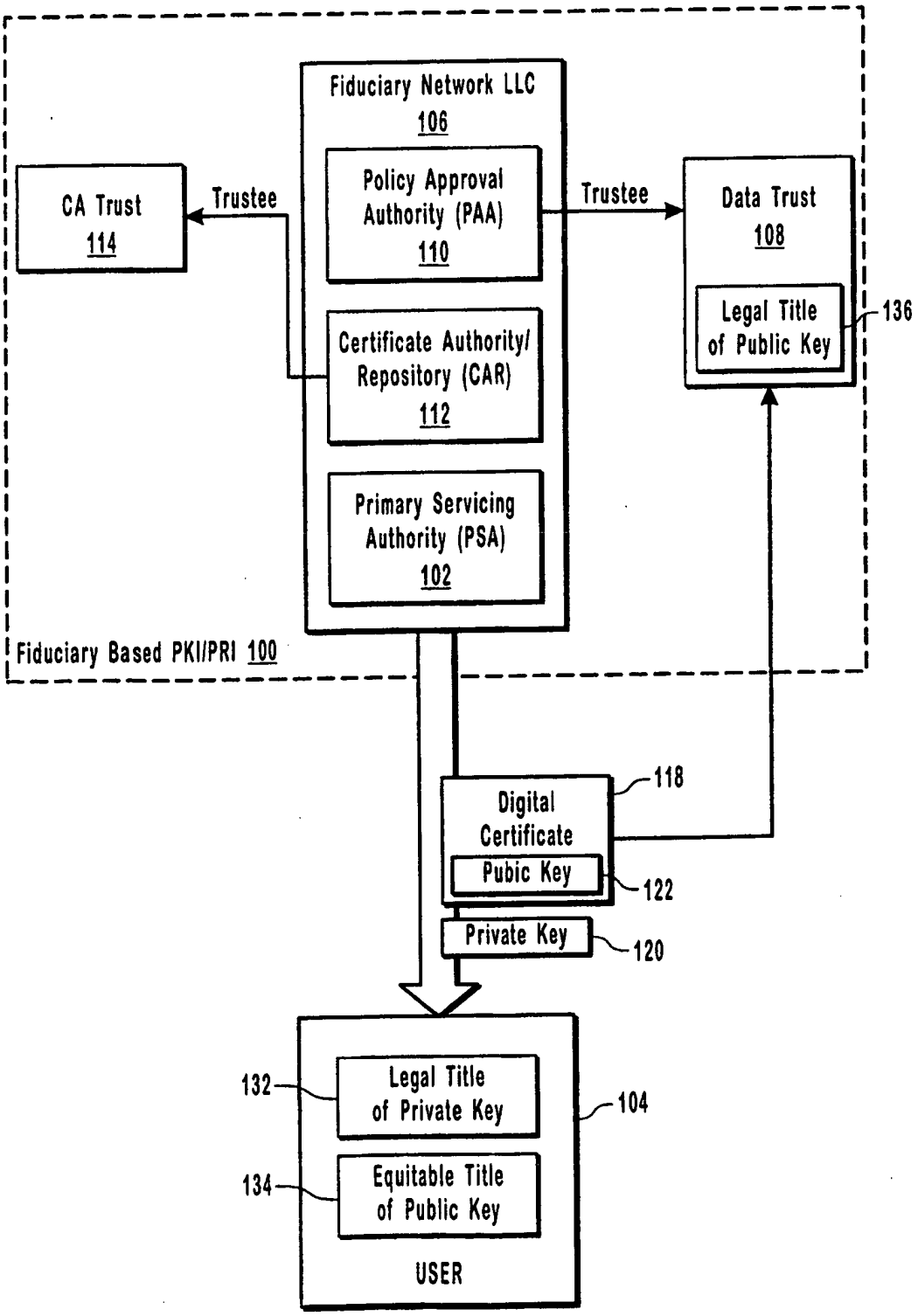

Fiduciary Network LLC
106
Policy Approval Authority (PAA)
110
Certificate Authority/ Repository (CAR)
112
Primary Servicing Authority (PSA)
102
CA Trust
114
Trustee
Trustee
Data Trust
108
Legal Title of Public Key
136
Fiduciary Based PKI/PRI 100
Digital Certificate
118
Pubic Key
122
Private Key
120
Legal Title of Private Key
132
Equitable Title of Public Key
134
USER
104

FIG. 5

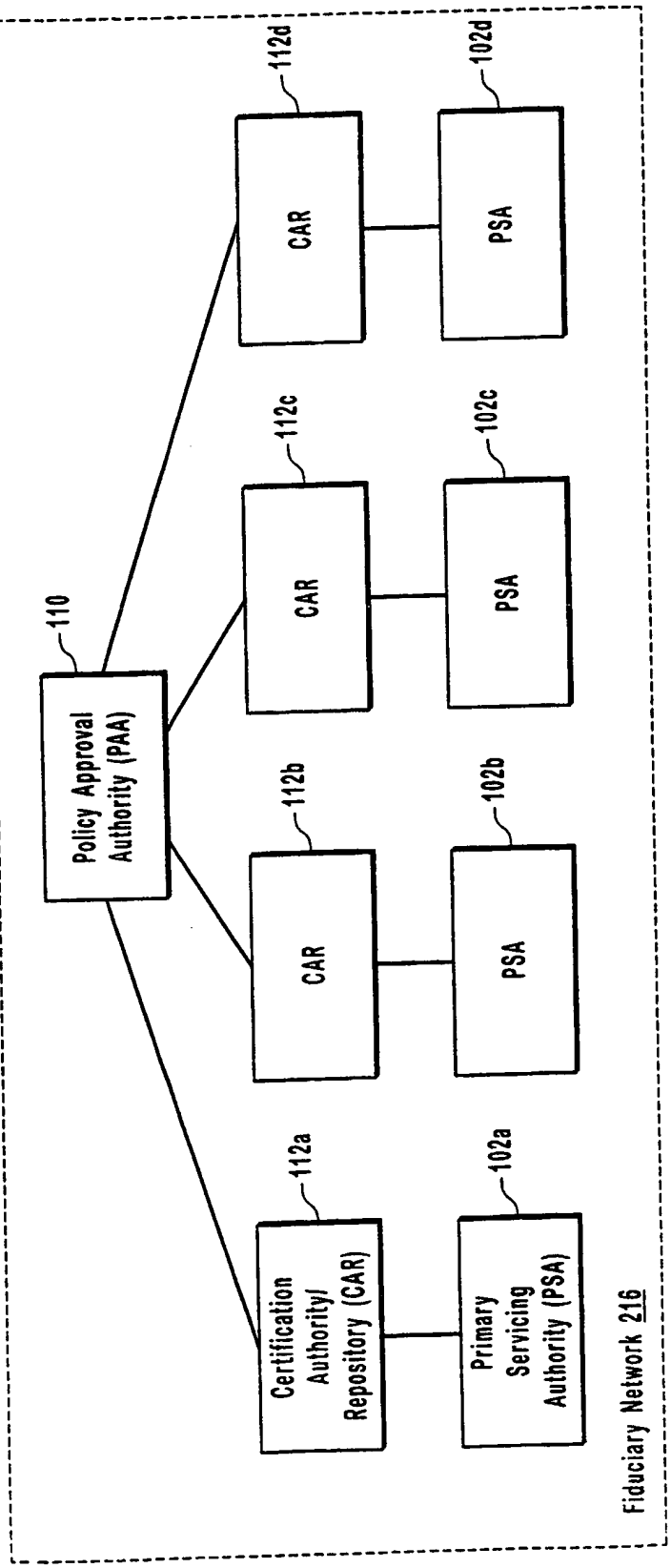

Fiduciary Network 216
Policy Approval Authority (PAA)
110
Certification Authority/ Repository (CAR)
112a
Primary Servicing Authority (PSA)
102a
CAR
112b
PSA
102b
CAR
112c
PSA
102c
CAR
112d
PSA
102d

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/30671

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 17/00, 17/30, 13/00, 12/00; H04L 9/00
US CL :707/9, 10, 203; 711/216; 380/4
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 707/9, 10, 203; 395/421.06; 380/4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,481,700 A (THURAISINGHAM) 02 January 1996, the entire paper is relevant	1, 13, 19, and 25
A	US 5,649,187 A (HORNBUCKLE) 15 July 1997, the entire paper is relevant	1-30
Y	US 5,694,569 A (FISCHER) 02 December 1997, the entire paper is relevant	1, 13, 19, and 25
Y	US 5,606,609 A (HOUSER et al.) 25 February 1997, the entire paper is elevant	1,13,19, and 25
Y	US 5,826,268 A (SCHAEFER ET AL.) 20 October 1998, the entire paper is relevant	1,13, 19, and 25

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 14 DECEMBER 2000	Date of mailing of the international search report 22 FEB 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer THUY PARDO Telephone No. (703) 305-9707

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/30671

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,920,861 A (HALL et al.) 06 July 1999, the entire paper is relevant	1,13, 19, and 25
A	US 5,966,715 A (SWEENEY et al.) 12 October 1999, the entire paper is relevant	1-30